**ФЕДЕРАЛЬНОЕ УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЪЕДИНЕНИЕ**

**В СИСТЕМЕ ВЫСШЕГО ОБРАЗОВАНИЯ ПО УКРУПНЕННОЙ ГРУППЕ СПЕЦИАЛЬНОСТЕЙ И НАПРАВЛЕНИЙ ПОДГОТОВКИ**

**10.00.00 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»**

****

УТВЕРЖДАЮ

Председатель ФУМО ВО ИБ

А.Б. Пичкур

30 ноября 2021 г.

**Методические рекомендации**

**по разработке основной профессиональной образовательной программы   
высшего образования**

Специальность

**10.05.02 Информационная безопасность телекоммуникационных систем**

Уровень высшего образования

**Специалитет**

Москва, 2021 г.

СОДЕРЖАНИЕ

# Раздел 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Назначение примерной основной образовательной программы

1.2. Нормативные документы

1.3. Перечень сокращений

# Раздел 2. ХАРАКТЕРИСТИКА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ ВЫПУСКНИКОВ

2.1. Общее описание профессиональной деятельности выпускников

2.2. Перечень профессиональных стандартов, соотнесенных с ФГОС ВО

2.3. Перечень основных задач профессиональной деятельности выпускников (по типам)

Раздел 3. ОБЩАЯ ХАРАКТЕРИСТИКА ОБРАЗОВАТЕЛЬНЫХ ПРОГРАММ, РЕАЛИЗУЕМЫХ В РАМКАХ СПЕЦИАЛЬНОСТИ

3.1. Направленности (профили) образовательных программ в рамках специальности

3.2. Квалификация, присваиваемая выпускникам образовательных программ

3.3. Объем программы

3.4. Формы обучения

3.5. Срок получения образования

Раздел 4. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

4.1. Перечень обязательных компетенций выпускников

4.2. Перечень рекомендуемых профессиональных компетенции выпускников

4.3. Индикаторы достижения компетенций

Раздел 5. ПРИМЕРНАЯ СТРУКТУРА И СОДЕРЖАНИЕ ОПОП

5.1. Рекомендуемый объем обязательной части образовательной программы

5.2. Рекомендуемые типы практики

5.3. Примерный учебный план и примерный календарный учебный график

5.4. Примерные программы дисциплин (модулей) и практик

5.5. Примерная рабочая программа воспитания

5.6. Примерный календарный план воспитательной работы

5.7. Рекомендации по разработке фондов оценочных средств для промежуточной аттестации по дисциплине (модулю) или практике

5.8. Рекомендации по разработке программы государственной итоговой аттестации

Раздел 6. ПРИМЕРНЫЕ УСЛОВИЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ ПО ОПОП

Раздел 7. СПИСОК РАЗРАБОТЧИКОВ

Приложение 1. Перечень профессиональных стандартов, соответствующих профессиональной деятельности выпускников, освоивших программу специалитета по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем»

Приложение 2. Перечень обобщённых трудовых функций и трудовых функций, имеющих отношение к профессиональной деятельности выпускника программы специалитета по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем»

Приложение 3. Примерный учебный план программы специалитета по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем»

Приложение 4. Примерный календарный учебный график программы специалитета по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем»

# Раздел 1. ОБЩИЕ ПОЛОЖЕНИЯ

**1.1. Назначение примерной основной образовательной программы**

Примерная основная образовательная программа (далее – ПООП) является комплексным методическим документом, рекомендованным организациям, осуществляющим образовательную деятельность по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем».

ПООП предназначена для разработки и реализации основных профессиональных образовательных программ высшего образования на основе федерального государственного образовательного стандарта высшего образования – специалитет по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем», утвержденного приказом Минобрнауки России   
от 26 ноября 2020 г. № 1458, зарегистрированного в Минюсте 15 февраля 2021 г., рег. № 62492 и с учётом профессиональных стандартов, сопряжённых   
с профессиональной деятельностью выпускников.

**1.2. Нормативные документы:**

* Федеральный закон от 29 декабря 2012 г. № 273-ФЗ «Об образовании   
  в Российской Федерации»;
* Федеральный государственный образовательный стандарт высшего образования – специалитет по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем», утвержденный приказом Минобрнауки России от 26 ноября 2020 г. № 1458, зарегистрированный в Минюсте 15 февраля 2021 г., рег. № 62492;
* Порядок организации и осуществления образовательной деятельности   
  по образовательным программам высшего образования – программам бакалавриата, программам магистратуры, программам специалитета, утвержденный приказом Минобрнауки России от 5 апреля 2017 г. № 301;
* Порядок организации и осуществления образовательной деятельности   
  по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры, утвержденный приказом Минобрнауки России от 6 апреля 2021 г. № 245;
* Порядок проведения государственной итоговой аттестации   
  по образовательным программам высшего образования – программам бакалавриата, программам специалитета и программам магистратуры, утвержденный приказом Минобрнауки России от 29 июня 2015 г. № 636 (в ред. приказа Минобрнауки России от 9 февраля 2016 г. № 86, от 27 марта 2020 г. № 490);
* Положение о практической подготовке обучающихся, утвержденное приказом Министерства науки и высшего образования Российской Федерации, Министерства просвещения Российской Федерации от 05.08.2020 № 885/390 (в ред. приказа Минобрнауки России № 1430, Минпросвещения России № 652 от 18 ноября 2020 г.).

**1.3. Перечень сокращений, используемых в тексте ПООП**

|  |  |  |
| --- | --- | --- |
| ЕКС | – | Единый квалификационный справочник; |
| з.е. | – | зачетная единица; |
| ОПК | – | общепрофессиональная компетенция; |
| ОПОП, образовательная программа | – | основная профессиональная образовательная программа по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем»; |
| Организация | – | организация, осуществляющая образовательную деятельность по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем»; |
| ОТФ | – | обобщённая трудовая функция; |
| ПД | – | профессиональная деятельность; |
| ПК | – | профессиональная компетенция; |
| ПС | – | профессиональный стандарт; |
| ПООП | – | примерная основная образовательная программа  по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем»; |
| программа специалитета | – | основная образовательная программа высшего образования – программа специалитета 10.05.02 «Информационная безопасность телекоммуникационных систем»; |
| сетевая форма | – | сетевая форма реализации образовательных программ; |
| СПК | – | Совет по профессиональным квалификациям; |
| УК | – | универсальная компетенция; |
| ФГОС ВО | – | федеральный государственный образовательный стандарт высшего образования по специальности  по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем»; |
| ФУМО | – | федеральное учебно-методическое объединение; |
| ФОС | – | фонд оценочных средств; |
| ИД | – | индикатор достижения; |
| ГИА | – | государственная итоговая аттестация; |
| ВКР | – | выпускная квалификационная работа. |

**Раздел 2. ХАРАКТЕРИСТИКА   
ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ ВЫПУСКНИКОВ**

**2.1. Общее описание профессиональной деятельности выпускников**

Области профессиональной деятельности и (или) сферы профессиональной деятельности, в которых выпускники, освоившие программу специалитета (далее – выпускники), могут осуществлять профессиональную деятельность:

01 Образование и наука (в сфере научных исследований);

06 Связь, информационные и коммуникационные технологии (в сфере разработки и обеспечения функционирования сетей электросвязи, средств и систем обеспечения защиты от несанкционированного доступа сетей электросвязи   
и циркулирующей в них информации);

12 Обеспечение безопасности (в сфере обеспечения функционирования   
и развития сетей связи специального назначения);

сфера обороны и безопасности;

сфера правоохранительной деятельности.

Выпускники могут осуществлять профессиональную деятельность в других областях профессиональной деятельности и (или) сферах профессиональной деятельности при условии соответствия уровня их образования и полученных компетенций требованиям к квалификации работника.

Типы задач профессиональной деятельности выпускников:

научно-исследовательский;

проектный;

контрольно-аналитический;

организационно-управленческий;

эксплуатационный.

При разработке и реализации программы специалитета Организация ориентируется на все типы задач профессиональной деятельности, к которым готовится специалист.

Перечень основных объектов (или областей знания) профессиональной деятельности выпускников по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем»:

методы, средства и системы обеспечения информационной безопасности телекоммуникационных сетей и систем;

управление информационной безопасностью телекоммуникационных сетей   
и систем;

информационно-телекоммуникационные сети и системы различного назначения, их оборудование, принципы построения.

**2.2. Перечень профессиональных стандартов, соотнесенных с ФГОС ВО**

Перечень профессиональных стандартов, соотнесенных с ФГОС ВО приведен в приложении 1.

Перечень обобщённых трудовых функций и трудовых функций, имеющих отношение к профессиональной деятельности выпускника программ специалитета по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем», представлен приложении 2.

**2.3. Перечень основных задач профессиональной деятельности выпускников, обобщённых трудовых функций и трудовых функций, имеющих отношение к профессиональной деятельности выпускника программ специалитета по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем».**

Соотнесение областей, типов задач и конкретных трудовых функций (обобщённых трудовых функций) профильного и смежных профессиональных стандартов, имеющих отношение к профессиональной деятельности выпускника   
по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем» приведены в таблице 1.

Таблица 1.

Соотнесение областей, типов задач и конкретных трудовых функций   
(обобщённых трудовых функций) профессиональных стандартов

| Область профессиональной деятельности  (по Реестру Минтруда) | Типы задач профессиональной деятельности | Коды трудовых функций  (задачи профессиональной деятельности) профессиональных стандартов |
| --- | --- | --- |
| Профильный профессиональный стандарт  «Специалист по защите информации в телекоммуникационных системах и сетях» | | |
| *01 Образование и наука (в сфере научных исследований)* | *научно-исследовательский* | D/03.7 Проведение научно-исследовательских и опытно-конструкторских работ в сфере разработки средств и систем защиты средств связи сетей электросвязи от несанкционированного доступа, создания защищенных телекоммуникационных систем. |
| *06 Связь, информационные и коммуникационные технологии (в сфере разработки и обеспечения функционирования сетей электросвязи, средств и систем обеспечения защиты от несанкционированного доступа сетей электросвязи и циркулирующей в них информации)* | *научно-исследовательский* | D/03.7 Проведение научно-исследовательских и опытно-конструкторских работ в сфере разработки средств и систем защиты средств связи сетей электросвязи от несанкционированного доступа, создания защищенных телекоммуникационных систем. |
| *проектный* | D/01.7 Анализ угроз информационной безопасности в сетях электросвязи.  D/02.7 Разработка средств и систем защиты средств связи сетей электросвязи от несанкционированного доступа, средств для поиска признаков компьютерных атак в сетях электросвязи защищенных телекоммуникационных систем. |
| *контрольно-аналитический* | B/01.6 Мониторинг функционирования средств связи сетей электросвязи, защищенности от несанкционированного доступа и компьютерных атак сооружений и средств связи сетей электросвязи. |
| *организационно-управленческий* | B/02.6 Управление функционированием средств связи сетей электросвязи, защищенностью от несанкционированного доступа и компьютерных атак сооружений и средств связи сетей электросвязи.  B/03.6 Управление персоналом, обслуживающим сооружения и средств связи сетей электросвязи, а также программные, программно-аппаратные (в том числе криптографические) и технические средства и системы их защиты от несанкционированного доступа, средства для поиска признаков компьютерных атак в сетях электросвязи.  F/01.7 Управление рисками систем защиты сетей электросвязи от несанкционированного доступа. |
| *эксплуатационный* | A/01.5 Установка программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты средств связи сетей электросвязи от несанкционированного доступа.  A/02.5 Обеспечение бесперебойной работы средств связи сетей электросвязи, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем их защиты от несанкционированного доступа.  A/03.5 Техническое обслуживание средств связи сетей электросвязи, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем их защиты от несанкционированного доступа. |
| *12 Обеспечение безопасности (в сфере обеспечения функционирования и развития сетей связи специального назначения)* | *научно-исследовательский* | E/02.7 Проведение научно-исследовательских и опытно-конструкторских работ в сфере разработки сетей связи специального назначения и их средств связи, включая средства криптографической защиты информации. |
| *контрольно-аналитический* | E/03.7 Контроль защищенности от несанкционированного доступа и функциональности сетей связи специального назначения. |
| *организационно-управленческий* | E/01.7 Организация функционирования сетей связи специального назначения и их средств связи. |
| *эксплуатационный* | C/01.6 Установка средств связи сетей связи специального назначения, включая средства криптографической защиты информации, средства для поиска признаков компьютерных атак в сетях электросвязи.  C/02.6 Обеспечение бесперебойной работы средств связи сетей связи специального назначения, включая средства криптографической защиты информации, средства для поиска признаков компьютерных атак в сетях электросвязи.  C/03.6 Ведение специального делопроизводства и технических документов в процессе эксплуатации средств связи сетей связи специального назначения, включая средства криптографической защиты информации. |
| Смежные профессиональные стандарты | | |
| *06 Связь, информационные и коммуникационные технологии (в сфере разработки и обеспечения функционирования сетей электросвязи, средств и систем обеспечения защиты от несанкционированного доступа сетей электросвязи и циркулирующей в них информации)* | *проектный* | 06.033 «Специалист по защите информации в автоматизированных системах»:  D/02.7 Разработка проектных решений по защите информации в автоматизированных системах.  D/04.7 Разработка программных и программно-аппаратных средств для систем защиты информации автоматизированных систем  06.034 «Специалист по технической защите информации»:  F/01.7 Проектирование средств и систем информатизации в защищенном исполнении.  F/02.7 Проектирование систем защиты информации на объектах информатизации.  06.006 «Специалист по радиосвязи и телекоммуникациям»:  A/02.6 Развитие коммутационных подсистем и сетевых платформ.  B/02.6 Развитие сетей радиодоступа.  C/02.6 Развитие транспортных сетей и сетей передачи данных.  C/03.6 Развитие спутниковых систем связи.  06.007 «Инженер-проектировщик в области связи (телекоммуникаций)»:  B/01.6 Разработка схемы организации связи объекта, телекоммуникационной системы.  B/02.6 Разработка проектной документации на объект (систему) связи, телекоммуникационную систему.  B/04.6 Выполнение специальных расчетов.  B/06.6. Проектирование систем станций подвижной радиосвязи.  B/07.6. Проектирование транспортной сети подвижной радиосвязи.  06.018 «Инженер связи (телекоммуникаций)»:  C/02.7 Разработка технической документации по эксплуатации оборудования связи (телекоммуникаций).  D/01.7 Сбор и анализ исходных данных для развития и оптимизации сети связи.  D/02.7 Формирование плана развития сети связи.  D/03.7 Выработка и внедрение решений по оптимизации сети связи. |
| *контрольно-аналитический* | 06.032 «Специалист по безопасности компьютерных систем и сетей»:  C/03.7 Проведение анализа безопасности компьютерных систем.  C/05.7 Проведение инструментального мониторинга защищенности компьютерных систем и сетей.  06.033 «Специалист по защите информации в автоматизированных системах»:  B/05.6 Мониторинг защищенности информации в автоматизированных системах.  B/06.6 Аудит защищенности информации в автоматизированных системах.  C/03.6 Анализ уязвимостей внедряемой системы защиты информации.  06.034 «Специалист по технической защите информации»:  G/01.7 Проведение аттестации объектов вычислительной техники на соответствие требованиям по защите информации.  06.018 «Инженер связи (телекоммуникаций)»:  A/03.6 Тестирование оборудования, отработка режимов работы, контроль проектных параметров работы оборудования связи (телекоммуникаций).  B/01.6 Проведение измерений параметров и проверки качества работы оборудования связи (телекоммуникаций).  B/04.6 Мониторинг состояния оборудования, учет отказов оборудования, ведение документации.  06.027 «Специалист по администрированию сетевых устройств информационно-коммуникационных систем»:  B/03.5 Оценка эффективности конфигурации сетевых устройств с точки зрения производительности сети и защиты от несанкционированного доступа.  D/01.6 Определение параметров безопасности и защиты программного обеспечения сетевых устройств. |
| *организационно-управленческий* | 06.031 «Специалист по автоматизации информационно-аналитической деятельности в сфере безопасности»:  D/03.7 Организация работ по выполнению в информационно-аналитических системах в защищенном исполнении требований защиты информации ограниченного доступа.  06.032 «Специалист по безопасности компьютерных систем и сетей»:  C/02.7 Разработка требований по защите, формирование  политик безопасности компьютерных систем и сетей.  D/03.7 Разработка эксплуатационной документации на системы защиты информации автоматизированных систем.  06.033 «Специалист по защите информации в автоматизированных системах»:  B/03.6 Управление защитой информации в автоматизированных системах.  C/02.6 Разработка организационно-распорядительных документов по защите информации в автоматизированных системах.  C/04.6 Внедрение организационных мер по защите информации в автоматизированных системах. |
| *эксплуатационный* | 06.031 «Специалист по автоматизации информационно-аналитической деятельности в сфере безопасности»:  C/03.7 Обеспечение функционирования средств защиты информации в информационно-аналитических систем в защищенном исполнении.  06.032 «Специалист по безопасности компьютерных систем и сетей»:  B/01.6 Администрирование подсистем защиты информации в операционных системах.  B/02.6 Администрирование программно-аппаратных средств защиты информации в компьютерных сетях.  B/03.6 Администрирование средств защиты информации прикладного и системного программного обеспечения.  06.033 «Специалист по защите информации в автоматизированных системах»:  B/02.6 Администрирование систем защиты информации автоматизированных систем.  C/01.6 Установка и настройка средств защиты информации в автоматизированных системах.  06.034 «Специалист по технической защите информации»:  B/01.6 Проведение работ по установке, настройке и испытаниям защищенных технических средств обработки информации.  06.006 «Специалист по радиосвязи и телекоммуникациям»:  A/01.6 Эксплуатация коммутационных подсистем и сетевых платформ.  B/01.6 Эксплуатация сетей радиодоступа.  C/01.6 Эксплуатация транспортных сетей и сетей передачи данных.  06.018 «Инженер связи (телекоммуникаций)»:  A/02.6 Настройка, регулировка и испытания оборудования связи (телекоммуникаций).  B/02.6 Проведение планово-профилактических работ.  B/03.6 Проведение ремонтно-восстанови тельных работ.  06.023«Работник по представлению услуг телефонной, телеграфной и радиосвязи»:  C/02.3 Эксплуатационно-техническое обслуживание оборудования приемо-передающих радиостанций.  06.027 «Специалист по администрированию сетевых устройств информационно-коммуникационных систем»:  A/01.4 Установка активных сетевых устройств.  A/02.4 Настройка программного обеспечения сетевых устройств.  A/03.4 Установка специальных средств управления сетевыми устройствами.  B/01.5 Настройка параметров сетевых устройств и программного обеспечения согласно технологической политике организации.  D/02.6 Установка специальных средств управления безопасностью администрируемой сети.  D/03.6 Администрирование средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов).  E/01.6 Выполнение регламентных работ по поддержке операционных систем сетевых устройств инфокоммуникационной системы.  E/03.6 Восстановление параметров программного обеспечения сетевых устройств.  F/01.7 Устранение сбоев и отказов сетевых устройств и операционных систем.  F/03.7 Устранение ошибок сетевых устройств и операционных систем. |

**Раздел 3. ОБЩАЯ ХАРАКТЕРИСТИКА ОБРАЗОВАТЕЛЬНЫХ ПРОГРАММ, РЕАЛИЗУЕМЫХ В РАМКАХ СПЕЦИАЛЬНОСТИ**

**3.1. Направленности (профили) образовательных программ в рамках специальности**

При разработке программы специалитета Организация выбирает специализацию программы специалитета из следующего перечня:

специализация № 1 «Мониторинг в телекоммуникационных системах»;

специализация № 2 «Системы представительской связи»;

специализация № 3 «Сети специальной связи»;

специализация № 4 «Системы и сети связи специального назначения»;

специализация № 5 «Системы специальной связи и информации для органов государственной власти»;

специализация № 6 «Информационная безопасность аэрокосмических телекоммуникационных систем»;

специализация № 7 «Разработка защищенных телекоммуникационных систем»;

специализация № 8 «Защита информации в радиосвязи и телерадиовещании»;

специализация № 9 «Управление безопасностью телекоммуникационных систем и сетей»;

специализация № 10 «Информационная безопасность мультисервисных телекоммуникационных сетей и систем на транспорте» (по видам);

специализация № 11 «Системы подвижной цифровой защищенной связи»;

специализация № 12 «Техническая защита информации информационно-телекоммуникационных систем».

Программы специалитета по специализациям № 1 «Мониторинг   
в телекоммуникационных системах», № 2 «Системы представительской связи», № 3 «Сети специальной связи», № 4 «Системы и сети связи специального назначения», № 5 «Системы специальной связи и информации для органов государственной власти» определяются квалификационными требованиями к военно-профессиональной подготовке, специальной профессиональной подготовке выпускников, устанавливаемыми федеральным государственным органом,   
в ведении которого находятся соответствующие организации.

**3.2. Квалификация, присваиваемая выпускникам образовательных программ:** специалист по защите информации.

**3.3. Объем программы:** 330 з.е.

**3.4. Формы обучения:** очная.

**3.5. Срок получения образования**

Срок получения образования по программе специалитета (вне зависимости   
от применяемых образовательных технологий):

в очной форме обучения, включая каникулы, предоставляемые после прохождения государственной итоговой аттестации, составляет 5,5 лет;

при обучении по индивидуальному учебному плану инвалидов и лиц   
с ограниченными возможностями здоровья может быть увеличен по их заявлению не более чем на 1 год по сравнению со сроком получения образования, установленным для очной формы обучения.

В федеральных государственных организациях, осуществляющих подготовку кадров в интересах обороны и безопасности государства, обеспечения законности   
и правопорядка, срок обучения по программе специалитета в связи   
с продолжительностью каникулярного времени обучающихся составляет не менее   
5 лет.

**Раздел 4. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ**

**4.1. Перечень компетенций выпускников**

Перечень универсальных компетенций:

УК-1. Способность осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий;

УК-2. Способность управлять проектом на всех этапах его жизненного цикла;

УК-3. Способность организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели;

УК-4. Способность применять современные коммуникативные технологии,   
в том числен на иностранном(ых) языке(ах), для академического   
и профессионального взаимодействия;

УК-5. Способность анализировать и учитывать разнообразие культур   
в процессе межкультурного взаимодействия;

УК-6. Способность определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни;

УК-7. Способность поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности;

УК-8. Способность создавать и поддерживать в повседневной жизни   
и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов;

УК-10. Способность принимать обоснованные экономические решения   
в различных областях жизнедеятельности;

УК-11. Способность формировать нетерпимое отношение к коррупционному поведению.

Перечень общепрофессиональных компетенций:

ОПК-1. Способность оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;

ОПК-2. Способность применять информационно-коммуникационные технологии, программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности;

ОПК-3. Способность использовать математические методы, необходимые   
для решения задач профессиональной деятельности;

ОПК-4. Способность анализировать физическую сущность явлений   
и процессов, лежащих в основе функционирования радиоэлектронной техники, применять физические законы и модели для решения задач профессиональной деятельности;

ОПК-5. Способность применять нормативные правовые акты, нормативные   
и методические документы, регламентирующие деятельность по защите информации;

ОПК-6. Способность при решении профессиональных задач организовывать защиту информации ограниченного доступа в процессе функционирования сетей электросвязи в соответствии с нормативными правовыми актами, нормативными   
и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

ОПК-7. Способность создавать программы на языке высокого уровня, применять существующие реализации структур данных и алгоритмов;

ОПК-8. Способность применять методы научных исследований при проведении разработок в области функционирования, развития и обеспечения информационной безопасности телекоммуникационных систем и сетей;

ОПК-9. Способность использовать программные, программно-аппаратные   
и технические средства защиты информации при решении задач профессиональной деятельности;

ОПК-10. Способность использовать методы и средства криптографической защиты информации при решении задач профессиональной деятельности;

ОПК-11. Способность применять положения теории в области электрических цепей, радиотехнических сигналов, распространения радиоволн, кодирования, электрической связи, цифровой обработки сигналов для решения задач профессиональной деятельности;

ОПК-12. Способность формулировать задачи, планировать и проводить исследования, в том числе эксперименты и математическое моделирование объектов, явлений и процессов телекоммуникационных систем, включая обработку и оценку достоверности их результатов;

ОПК-13. Способность оценивать технические возможности, анализировать угрозы и вырабатывать рекомендации по построению элементов информационно-телекоммуникационной инфраструктуры с учетом обеспечения требований информационной безопасности;

ОПК-14. Способность применять технологии и технические средства сетей электросвязи;

ОПК-15. Способность проводить инструментальный мониторинг качества обслуживания и анализ защищенности информации от несанкционированного доступа в телекоммуникационных системах и сетях в целях управления   
их функционированием;

ОПК-16. Способность проектировать защищённые телекоммуникационные системы и их элементы, проводить анализ проектных решений по обеспечению заданного уровня безопасности и требуемого качества обслуживания телекоммуникационных систем, разрабатывать необходимую техническую документацию с учетом действующих нормативных и методических документов, проводить подготовку исходных данных для технико-экономического обоснования соответствующих проектных решений;

ОПК-17. Способность анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории,   
в том числе для формирования гражданской позиции и развития патриотизма.

Перечень общепрофессиональных компетенций по специализациям

Специализация № 6 «Информационная безопасность аэрокосмических телекоммуникационных систем»:

ОПК-6.1. Способность выбирать методы и разрабатывать средства защиты объектов аэрокосмических телекоммуникационных систем при воздействии радиопомех;

ОПК-6.2. Способность проектировать системы защищенного информационного взаимодействия объектов аэрокосмического и наземного сегментов;

ОПК-6.3. Способность разрабатывать инфокоммуникационные системы, энергетически эффективно и скрытно использующие радиоканал   
для информационного взаимодействия;

Специализация № 7 «Разработка защищенных телекоммуникационных систем»:

ОПК-7.1. Способность формировать техническое задание и разрабатывать аппаратное и программное обеспечение компонентов защищенных телекоммуникационных систем;

ОПК-7.2. Способность участвовать в разработке систем управления информационной безопасностью телекоммуникационных систем;

ОПК-7.3. Способность обеспечивать защиту программных средств защищенных телекоммуникационных систем;

Специализация № 8 «Защита информации в радиосвязи и телерадиовещании»:

ОПК-8.1. Способность осуществлять частотно-территориальное и кодовое планирование сетей радиосвязи и телерадиовещания;

ОПК-8.2. Способность применять методы приема, передачи и обработки сигналов, обеспечивающие повышение эффективности и защищенности систем радиосвязи и телерадиовещания;

ОПК-8.3. Способность разрабатывать системы, сети и устройства защищенной радиосвязи и телерадиовещания;

Специализация № 9 «Управление безопасностью телекоммуникационных систем и сетей»:

ОПК-9.1. Способность формировать, внедрять и обеспечивать функционирование системы менеджмента информационной безопасности телекоммуникационных систем и сетей;

ОПК-9.2. Способность реализовывать комплекс организационных мероприятий по обеспечению информационной безопасности и устойчивости телекоммуникационных систем и сетей;

ОПК-9.3. Способность проводить мониторинг защищенности сетевых ресурсов и формировать отчеты по выявленным уязвимостям;

Специализация № 10 «Информационная безопасность мультисервисных телекоммуникационных систем и сетей транспорта (по видам) и оценивать   
их эффективность»:

ОПК-10.1. Способность проводить теоретические и экспериментальные исследования телекоммуникационных систем и сетей транспорта (по видам)   
и оценивать их эффективность;

ОПК-10.2. Способность осуществлять рациональный выбор методов и средств обеспечения информационной безопасности мультисервисных телекоммуникационных систем и сетей транспорта (по видам);

ОПК-10.3. Способность использовать методы и средства измерений   
для решения метрологических задач и технической диагностики защищенных систем и сетей транспорта (по видам);

Специализация № 11 «Системы подвижной цифровой защищенной связи»:

ОПК-11.1. Способность выбирать методы, разрабатывать и реализовывать алгоритмы для обеспечения безопасности систем подвижной цифровой защищенной связи;

ОПК-11.2. Способность контролировать работоспособность и оценивать эффективность средств защиты информации в системах подвижной цифровой защищенной связи;

ОПК-11.3. Способность использовать и реализовывать алгоритмы распределенной обработки информации и сигналов в целях обеспечения безопасности систем подвижной цифровой защищенной связи;

Специализация № 12 «Техническая защита информации информационно-телекоммуникационных систем»:

ОПК-12.1. Способность проектировать системы технической защиты информации для объектов информатизации;

ОПК-12.2. Способность проектировать средства и системы информатизации   
в защищенном исполнении;

ОПК-12.3. Способность проводить аттестацию объектов информатизации   
на соответствие требованиям по защите информации.

Профессиональные компетенции определяются Организацией самостоятельно на основе профессиональных стандартов, соответствующих профессиональной деятельности выпускников (при наличии).

При определении профессиональных компетенций на основе профессиональных стандартов Организация осуществляет выбор профессиональных стандартов, соответствующих профессиональной деятельности выпускников,   
из числа указанных в приложении 1 и (или) иных профессиональных стандартов, соответствующих профессиональной деятельности выпускников, из реестра профессиональных стандартов (перечня видов профессиональной деятельности), размещенного на специализированном сайте Министерства труда и социальной защиты Российской Федерации «Профессиональные стандарты» (<http://profstandart.rosmintrud.ru>) (при наличии соответствующих профессиональных стандартов).

Из каждого выбранного профессионального стандарта Организация выделяет одну или несколько ОТФ, соответствующих профессиональной деятельности выпускников, на основе установленных профессиональным стандартом для ОТФ уровня квалификации и требований раздела «Требования к образованию   
и обучению». ОТФ может быть выделена полностью или частично.

При отсутствии профессиональных стандартов, соответствующих профессиональной деятельности выпускников, профессиональные компетенции определяются Организацией на основе анализа требований к профессиональным компетенциям, предъявляемых к выпускникам на рынке труда, обобщения отечественного и зарубежного опыта, проведения консультаций с ведущими работодателями, объединениями работодателей отрасли, в которой востребованы выпускники, иных источников.

В федеральных государственных организациях, осуществляющих подготовку кадров в интересах обороны и безопасности государства, обеспечения законности   
и правопорядка, перечень профессиональных компетенций, формируемых в рамках специализаций № 1 «Мониторинг в телекоммуникационных системах», № 2 «Системы представительской связи», № 3 «Сети специальной связи», № 4 «Системы и сети связи специального назначения», № 5 «Системы специальной связи   
и информации для органов государственной власти», определяется на основе квалификационных требований к военно-профессиональной, специальной профессиональной подготовке выпускников, устанавливаемых федеральным государственным органом, в ведении которого находятся соответствующие организации.

**4.2. Индикаторы достижения компетенций выпускников**

Перечень индикаторов достижения универсальных и общепрофессиональных компетенций выпускников, соотнесенных с компетенциями, приведен в таблице 2.

Организация вправе дополнить указанный перечень индикаторами, разработанными самостоятельно.

Индикаторы достижения профессиональных компетенций выпускников Организация разрабатывает самостоятельно.

Таблица 2.

Универсальные и общепрофессиональные компетенции выпускников и индикаторы их достижения   
по специальности 10.05.02 Информационная безопасность телекоммуникационных систем

| **Код и наименование компетенции** | **Код  индикатора** | **Индикаторы достижения компетенции** | **Наименование учебной, дисциплины (модуля), практики, НИР, ВКР, формирующие компетенцию  по примерному учебному плану** | **Код ПС  (код ОТФ, ТФ,)  при наличии** |
| --- | --- | --- | --- | --- |
| **Универсальные компетенции (УК)** | | | | |
| **УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий** | УК-1.1.1 | знает содержание и взаимосвязь основных принципов, законов, понятий и категорий философских наук, основные этапы развития философской мысли, основную проблематику и структуру философского знания | Философия |  |
| УК-1.1.2 | знает понятие мировоззрения, исторические типы мировоззрения, соотношение философии и мировоззрения, соотношение философского мировоззрения и научной картины мира |
| УК-1.1.3 | знает основные источники информации о проблемных ситуациях в профессиональной деятельности и подходы к критическому анализу этой информации | Управление проектами |
| УК-1.1.4 | знает порядок принятия решений при возникновении проблемных ситуаций в профессиональной деятельности |
| УК-1.2.1 | умеет критически анализировать проблемные ситуации и вырабатывать стратегию действий в ходе решения профессиональных задач |
| **УК-2. Способен управлять проектом на всех этапах его жизненного цикла** | УК-2.1.1 | знает основные модели жизненного цикла проекта, его этапы и фазы, их характеристики и особенности | Управление проектами |  |
| УК-2.2.1 | умеет разрабатывать и реализовывать этапы проекта в сфере профессиональной деятельности |
| **УК-3. Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели** | УК-3.1.1 | знает содержание организации и руководства деятельностью рабочего коллектива (группы) | Управление проектами |  |
| УК-3.1.2 | знает социально-психологические характеристики рабочего коллектива (группы) |
| УК-3.1.3 | знает основы поддержания нравственных отношений в рабочем коллективе (группе) |
| УК-3.2.1 | умеет организовывать работу коллектива (группы) для решения поставленных задач в сфере профессиональной деятельности |
| **УК-4. Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия** | УК-4.1.1 | знает языковые нормы, правила составления и оформления различных служебных документов и научных текстов, а также формулы речевого этикета в профессиональном общении | Дисциплина (модуль) части, формируемой участниками образовательных отношений |  |
| УК-4.1.2 | знает основные фонетические особенности, лексический минимум, грамматический строй иностранного языка для устной и письменной коммуникации в сфере профессиональной деятельности | Иностранный язык |
| УК-4.2.1 | умеет составлять тексты различных типов в сфере профессиональной деятельности в соответствии с языковыми нормами, особенностями функциональных стилей речи и установленными стандартами | Производственная (преддипломная) практика |
| УК-4.2.2 | умеет вести диалогическую и монологическую речь в основных ситуациях профессионального общения на иностранном языке, читать и переводить (со словарем) тексты, извлекать и использовать в профессиональной деятельности полученную информацию | Иностранный язык |
| **УК-5. Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия** | УК-5.1.1 | знает особенности культуры народов России и основных мировых цивилизаций, особенности мировых и основных национальных религий, влияющие на взаимодействие в профессиональной деятельности | Дисциплина (модуль) части, формируемой участниками образовательных отношений |  |
| УК-5.2.1 | умеет учитывать национальные, этнокультурные и конфессиональные особенности при взаимодействии в профессиональной деятельности |
| **УК-6. Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни** | УК-6.1.1 | знает методы и средства самостоятельного решения задач в сфере профессиональной деятельности | Управление проектами |  |
| УК-6.1.2 | знает основы деятельностного подхода |
| УК-6.2.1 | умеет определять приоритеты профессиональной деятельности и способы ее совершенствования на основе самооценки | Производственная (преддипломная) практика |
| УК-6.2.2 | умеет планировать самостоятельную деятельность в решении профессиональных задач |
| **УК-7. Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности[[1]](#footnote-1)** | УК-7.1.1 | знает основы теории и методики физического воспитания | Физическая культура |  |
| УК-7.1.2 | знает основы организации и проведения самостоятельных занятий по физической подготовке |
| УК-7.2.1 | умеет переносить физическую нагрузку и психологическое напряжение, возникающее в связи с ней |
| **УК-8. Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов1** | УК-8.1.1 | знает опасные и вредные факторы системы «человек – среда обитания», факторы, угрожающие жизни человека в условиях чрезвычайных ситуаций и военных конфликтов | Безопасность жизнедеятельности[[2]](#footnote-2) |  |
| УК-8.1.2 | знает основные требования по охране окружающей среды, по охране труда и технике безопасности в профессиональной деятельности и в повседневной жизни, основные приемы оказания первой помощи |
| УК-8.2.2 | умеет использовать средства индивидуальной защиты, оказывать первую помощь при ранениях и травмах в повседневной деятельности, в условиях чрезвычайных ситуаций и военных конфликтов |
| **УК-10. Способен принимать обоснованные экономические решения в различных областях жизнедеятельности** | УК-10.1.1 | знает основные виды доходов, финансовые инструменты, виды и источники возникновения экономических и финансовых рисков в экономике | Экономика |  |
| УК-10.1.2 | знает место, роль и функции государства в экономике, цели, задачи и инструменты бюджетно-налоговой, денежно-кредитной политики государства и их влияние на макроэкономические параметры и поведение индивидов |
| УК-10.1.3 | знает нормативные правовые акты, регламентирующие вопросы реализации бюджетно-налоговой и денежно-кредитной политики государства |
| УК-10.2.1 | умеет анализировать информацию, необходимую для принятия обоснованных экономических решений, уметь прогнозировать их последствия и применять полученные знания в сфере личного экономического и финансового планирования |
| УК-10.2.2 | умеет применять нормативные правовые акты при принятии экономических решений |
| **УК-11. Способен формировать нетерпимое отношение к коррупционному поведению** | УК-11.1.1 | знает содержание основных нормативных правовых актов в сфере противодействия коррупции | Дисциплина (модуль) части, формируемой участниками образовательных отношений |  |
| УК-11.2.2 | умеет соблюдать требования антикоррупционного законодательства, воздерживаться от поведения, вызывающего сомнение в объективном и беспристрастном исполнении должностных (служебных) обязанностей |
| **Общепрофессиональные компетенции (ОПК)** | | | | |
| **ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства** | ОПК-1.1.1 | знает место и роль информационной безопасности в системе национальной безопасности Российской Федерации | Основы информационной безопасности |  |
| ОПК-1.1.2 | знает сущность и понятие информационной безопасности, характеристику ее составляющих |
| **ОПК-2. Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности** | ОПК-2.1.1 | знает классификацию компьютерных систем, виды информационного взаимодействия и обслуживания, основы построения информационно-вычислительных систем | Прикладные информационные технологии | **ПС 06.027**  ОТФ A  ТФ A/02.4  **ПС 06.007**  ОТФ B  ТФ B/03.6 |
| ОПК-2.1.2 | знает назначение, функции и обобщённую структуру операционных систем и типовые операционные системы, в том числе отечественного производства |
| ОПК-2.1.3 | знает типовые прикладные информационные технологии и программное обеспечение, используемое для решения задач профессиональной деятельности, в том числе системы баз данных, технологии распределенного реестра и искусственного интеллекта |
| ОПК-2.2.1 | умеет применять выбранные информационные технологии, программные средства системного и прикладного назначений для решения задач профессиональной деятельности |
| **ОПК-3. Способен использовать математические методы, необходимые для решения задач профессиональной деятельности** | ОПК-3.1.1 | знает основные положения теории пределов функций, теории рядов | Математический анализ |  |
| ОПК-3.1.2 | знает основные теоремы дифференциального и интегрального исчисления функций одного и нескольких переменных |
| ОПК-3.1.3 | знает основные теоремы теории функций комплексного переменного |
| ОПК-3.2.1 | умеет решать типовые задачи на вычисление пределов функций, дифференцирование и интегрирование, на разложение функций в ряды |
| ОПК-3.2.2 | умеет производить исследование функций, применять приложения дифференциального и интегрального исчисления |
| ОПК-3.2.3 | умеет применять аппарат теории функций комплексного переменного, в том числе для решения задач в действительной области |
| ОПК-3.1.4 | знает основные положения теории матриц, методы решения систем линейных уравнений | Алгебра и геометрия |
| ОПК-3.1.5 | знает основные понятия аналитической геометрии |
| ОПК-3.1.6 | знает основные алгебраические структуры и методы работы с ними |
| ОПК-3.1.7 | знает основные понятия векторной алгебры, в том числе линейные векторные и евклидовые пространства и их линейные преобразования |
| ОПК-3.2.4 | умеет пользоваться методами описания объектов средствами аналитической геометрии |
| ОПК-3.2.5 | умеет использовать основные методы линейной и общей алгебры для решения типовых задач дискретной математики |
| ОПК-3.1.8 | знает основные положения и методы комбинаторики, теории графов и элементы теории булевых функции | Дискретная математика |
| ОПК-3.1.9 | знает элементы теории кодов и теории автоматов |
| ОПК-3.2.6 | умеет пользоваться методами дискретной математики для решения задач профессиональной деятельности |
| ОПК-3.1.10 | знает основные понятия и методы теории вероятностей | Теория вероятностей и математическая статистика |
| ОПК-3.1.11 | знает основные функциональные и числовые характеристики распределений случайных величин и случайных векторов |
| ОПК-3.1.12 | знает различные формы предельных теорем и методы их доказательства |
| ОПК-3.1.13 | знает основные понятия и методы математической статистики |
| ОПК-3.1.14 | знает основные характеристики и методы построения статистических оценок параметров, доверительных интервалов и статистических критериев |
| ОПК-3.2.7 | умеет применять стандартные методы и модели к решению теоретико-вероятностных задач в профессиональной области, в том числе применять при решении прикладных задач аппарат вероятностных распределений случайных величин |
| ОПК-3.2.8 | умеет строить статистические модели экспериментов при решении прикладных задач, оценивать параметры статистических моделей, описывать и вычислять характеристики критериев проверки статистических гипотез |
| **ОПК-4. Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования радиоэлектронной техники, применять физические законы и модели для решения задач профессиональной деятельности** | ОПК-4.1.1 | знает основные законы механики | Физика |  |
| ОПК-4.1.2 | знает основные законы термодинамики и молекулярной физики |
| ОПК-4.1.3 | знает основные законы электричества и магнетизма |
| ОПК-4.1.4 | знает основы теории колебаний и волн, волновой оптики |
| ОПК-4.1.5 | знает основы квантовой оптики, квантовой механики |
| ОПК-4.2.1 | умеет использовать математические модели физических явлений и процессов |
| ОПК-4.2.2 | умеет решать типовые прикладные физические задачи |
| ОПК-4.2.3 | умеет проводить физический эксперимент, обрабатывать его результаты и делать выводы о проделанной исследовательской работе |
| ОПК-4.1.6 | знает принципы действия и характеристики электронных компонентов телекоммуникационных систем | Электроника и схемотехника |
| ОПК-4.1.7 | знает типовые схемотехнические решения основных узлов и блоков электронной аппаратуры |
| ОПК-4.1.8 | знает методы анализа электронных схем |
| ОПК-4.1.9 | знает основные правила выполнения и оформления электрических схем |
| ОПК-4.2.4 | умеет анализировать элементную базу электронной аппаратуры |
| ОПК-4.2.5 | умеет работать с программными средствами схемотехнического моделирования и использовать измерительную технику при экспериментальном исследовании электронной аппаратуры |
| **ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации** | ОПК-5.1.1 | знает нормативную правовую основу организации лицензирования отдельных видов деятельности в области защиты информации, сертификации средств защиты информации и аттестации объектов информатизации | Организационное и правовое обеспечение информационной безопасности |  |
| ОПК-5.1.2 | знает правовые основы организации защиты информации |
| ОПК-5.1.3 | знает правовую характеристику преступлений в сфере компьютерной информации и меры юридической ответственности за правонарушения и преступления в области защиты информации |
| ОПК-5.2.1 | умеет применять юридические понятия и термины, нормативные правовые акты и нормативные методические документы в области защиты информации |
| **ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в процессе функционирования сетей электросвязи в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю** | ОПК-6.1.1 | знает назначение, структуру и состав системы обеспечения информационной безопасности Российской Федерации | Организационное и правовое обеспечение информационной безопасности | **ПС 06.030**  ОТФ B  ТФ B/02.6, B/03.6  **ПС 06.031**  ОТФ D  ТФ D/03.7  **ПС 06.033**  ОТФ С  ТФ C/02.6, C/04.6 |
| ОПК-6.1.2 | знает организацию деятельности по обеспечению безопасности критически важной информационной инфраструктуры Российской Федерации, основные требования, предъявляемые к организации защиты информации ограниченного доступа в процессе функционирования сетей электросвязи |
| ОПК-6.1.3 | знает нормативные, руководящие и методические документы уполномоченных федеральных органов государственной власти по защите информации ограниченного доступа |
| ОПК-6.1.4 | знает задачи органов защиты государственной тайны и служб защиты информации на предприятиях |
| ОПК-6.1.5 | знает систему организационных мер, направленных на защиту информации ограниченного доступа |
| ОПК-6.1.6 | знает порядок организации защиты информации ограниченного доступа в процессе функционирования сетей электросвязи | Комплексное обеспечение защиты информации телекоммуникационных систем |
| ОПК-6.2.1 | умеет организовать защиту информации ограниченного доступа в процессе функционирования сетей электросвязи в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю |
| **ОПК-7. Способен создавать программы на языке высокого уровня, применять существующие реализации структур данных и алгоритмов** | ОПК-7.1.1 | знает представления данных в памяти компьютера | Языки программирования |  |
| ОПК-7.1.2 | знает основные конструкции и библиотеки языка программирования |
| ОПК-7.1.3 | знает принципы построения программ в процедурно-ориентированной и объектно-ориентированной парадигмах |
| ОПК-7.2.1 | умеет реализовывать алгоритмы на языке программирования |
| ОПК-7.2.2 | умеет работать с интегрированной средой разработки программного обеспечения |
| ОПК-7.2.3 | умеет использовать сторонние программные библиотеки |
| ОПК-7.3.1 | владеет навыками разработки и тестирования программ по поставленной спецификации |
| ОПК-7.1.4 | знает основные структуры данных, основные комбинаторные и теоретико-графовые алгоритмы | Методы программирования |
| ОПК-7.1.5 | знает методику оценки вычислительной сложности алгоритма |
| ОПК-7.1.6 | знает способы эффективной реализации алгоритмов |
| ОПК-7.2.4 | умеет проводить оценку вычислительной сложности алгоритма |
| ОПК-7.3.2 | владеет навыками выбора и разработки алгоритмов при решении типовых задач программирования |
| **ОПК-8. Способен применять методы научных исследований при проведении разработок в области функционирования, развития и обеспечения информационной безопасности телекоммуникационных систем и сетей** | ОПК-8.1.1 | знает основные формы, методы и приемы научного исследования, применяемые при проведении разработок в области функционирования, развития и обеспечения информационной безопасности телекоммуникационных систем и сетей | Проектирование защищенных телекоммуникационных систем | **ПС 06.030,**  ОТФ D  ТФ D/03.7 |
| ОПК-8.2.1 | умеет проводить исследования и эксперименты, оформлять отчеты при проведении разработок в области функционирования, развития и обеспечения информационной безопасности телекоммуникационных систем и сетей | Производственная (преддипломная) практика |
| **ОПК-9. Способен использовать программные, программно-аппаратные и технические средства защиты информации при решении задач профессиональной деятельности** | ОПК-9.1.1 | знает основные программные и программно-аппаратные средства защиты информации телекоммуникационных систем от несанкционированного доступа и принципы работы этих средств | Программно-аппаратные средства защиты информации телекоммуникационных систем | **ПС 06.030**  ОТФ A  ТФ A/01.5, A/02.5, A/03.5  **ПС 06.031**  ОТФ C  ТФ C/03.7  **ПС 06.032**  ОТФ B  ТФ B/01.6, B/02.6, B/03.6  **ПС 06.033**  ОТФ B  ТФ B/02.6  ОТФ С  ТФ C/01.6  **ПС 06.034**  ОТФ B  ТФ B/01.7  ОТФ F  ТФ F/02.7  **ПС 06.027**  ОТФ D  ТФ D/02.6, D/03.6 |
| ОПК-9.2.1 | умеет настраивать типовые программные и программно-аппаратные средства защиты информации телекоммуникационных систем от несанкционированного доступа |
| ОПК-9.1.2 | знает технические каналы утечки информации | Защита информации от утечки по техническим каналам |
| ОПК-9.1.3 | знает методы, способы и средства защиты информации от утечки по типовым техническим каналам на объектах информатизации |
| ОПК-9.2.2 | умеет проводить предпроектное обследование объекта информатизации с целью выявления потенциальных технических каналов утечки информации |
| ОПК-9.2.3 | умеет обосновывать рациональный состав средств защиты информации от утечки по техническим каналам для защиты объекта информатизации |
| ОПК-9.2.4 | умеет устанавливать и настраивать средства защиты информации от утечки по техническим каналам |
| **ОПК-10. Способен использовать методы и средства криптографической защиты информации при решении задач профессиональной деятельности** | ОПК-10.1.1 | знает основные понятия криптографии и криптографические методы защиты информации | Методы и средства криптографической защиты информации | **ПС 06.030,**  ОТФ A  ТФ A/01.5, A/02.5, A/03.5 |
| ОПК-10.1.2 | знает основные типы средств криптографической защиты информации и предъявляемые к ним требования |
| ОПК-10.1.3 | знает основные криптографические алгоритмы и механизмы, определяемые национальными стандартами и рекомендациями Российской Федерации и стандартами международной организации по стандартизации |
| ОПК-10.2.1 | умеет осуществлять обоснованный выбор и использовать средства криптографической защиты информации при решении задач профессиональной деятельности |
| **ОПК-11. Способен применять положения теории в области электрических цепей, радиотехнических сигналов, распространения радиоволн, кодирования, электрической связи, цифровой обработки сигналов для решения задач профессиональной деятельности** | ОПК-11.1.1 | знает устройство, принципы построения и работы, технические возможности и назначение, основные параметры и характеристики типовых электрических цепей | Теория электросвязи (Теория электрических цепей, Теория радиотехнических сигналов, Теория электрической связи, Теория информации и кодирования) | **ПС 06.030**  ОТФ D  ТФ D/02.7, D/03.7  **ПС 06.007**  ОТФ B  ТФ B/03.6 |
| ОПК-11.1.2 | знает методы анализа электрических цепей при постоянных напряжениях, гармонических и произвольных воздействиях |
| ОПК-11.2.1 | умеет рассчитывать основные параметры типовых электрических цепей в стационарных и переходных режимах процессов в них |
| ОПК-11.2.2 | умеет производить оценку и измерение отдельных характеристик типовых электрических цепей |
| ОПК-11.1.3 | знает основные математические модели, методы спектрального и корреляционного анализа сигналов, спектральные и корреляционные характеристики непрерывных и дискретных детерминированных сигналов |
| ОПК-11.1.4 | знает основные виды модуляции сигналов |
| ОПК-11.2.3 | умеет рассчитывать спектральные и корреляционные характеристики типовых детерминированных сигналов |
| ОПК-11.1.5 | знает способы представления сообщений, сигналов и помех, преобразования сигналов в каналах связи |
| ОПК-11.1.6 | знает основы оптимального приема сигналов в присутствии помех и типовые схемы оптимальных приемников |
| ОПК-11.2.4 | умеет выбирать статистические модели сигналов и помех, типовые схемы оптимальных приемников и оценивать помехоустойчивость оптимального приема типовых сигналов на фоне помех |
| ОПК-11.1.7 | знает основные понятия теории информации |
| ОПК-11.1.8 | знает основные коды источников информации и помехоустойчивые коды, основные параметры и способы представления помехоустойчивых кодов |
| ОПК-11.2.5 | умеет рассчитывать параметры помехоустойчивых кодов |
| ОПК-11.2.6 | умеет применять базовые способы кодирования и декодирования типовых помехоустойчивых кодов и кодов источников информации |
| ОПК-11.1.9 | знает физические основы излучения и распространения радиоволн в различных средах, а также особенности распространения радиоволн различных диапазонов частот | Антенны и распространение радиоволн |
| ОПК-11.1.10 | знает основные типы, принципы действия, характеристики и особенности антенн, линий передачи, элементов волноводной и фидерной техники, методы и приемы расчета их характеристик |
| ОПК-11.2.7 | умеет рассчитывать параметры типовых трасс распространения радиоволн |
| ОПК-11.2.8 | умеет рассчитывать характеристики типовых антенн, линий питания и отдельных устройств СВЧ |
| ОПК-11.1.11 | знает дискретные и цифровые сигналы и системы, способы их представления и описания, основные методы анализа дискретных сигналов и систем | Цифровая обработка сигналов |
| ОПК-11.1.12 | знает методы проектирования цифровых фильтров |
| ОПК-11.2.9 | умеет применять методы анализа и синтеза цифровых сигналов и систем для решения задач профессиональной деятельности |
| **ОПК-12. Способен формулировать задачи, планировать и проводить исследования, в том числе эксперименты и математическое моделирование объектов, явлений и процессов телекоммуникационных систем, включая обработку и оценку достоверности их результатов** | ОПК-12.1.1 | знает принципы и основные этапы математического и имитационного моделирования, походы к формализации явлений и процессов телекоммуникационных систем, типовые модели объектов, явлений и процессов телекоммуникационных систем | Моделирование систем и сетей телекоммуникаций | **ПС 06.030**  ОТФ D  ТФ D/03.7  **ПС 06.007**  ОТФ B  ТФ B/03.6 |
| ОПК-12.1.2 | знает основные возможности избранного средства моделирования объектов, явлений и процессов телекоммуникационных систем |
| ОПК-12.2.1 | умеет разрабатывать модели и проводить математическое и имитационное моделирование типовых объектов, явлений и процессов телекоммуникационных систем |
| ОПК-12.1.3 | знает принципы построения и работы измерительных устройств и приборов | Измерения в телекоммуникационных системах |
| ОПК-12.1.4 | знает методики обработки и оценки достоверности результатов измерений |
| ОПК-12.2.2 | умеет проводить измерения в спектральной и временной областях |
| **ОПК-13. Способен оценивать технические возможности, анализировать угрозы и вырабатывать рекомендации по построению элементов информационно-телекоммуникационной инфраструктуры с учетом обеспечения требований информационной безопасности** | ОПК-13.1.1 | знает эталонную модель взаимодействия открытых систем, основные протоколы и стандарты, используемые в сетях и системах электрической связи | Сети и системы передачи информации | **ПС 06.030**  ОТФ B  ТФ B/02.7  ОТФ D  ТФ D/01.7, D/02.7  **ПС 06.032**  ОТФ C  ТФ C/02.7, C/03.7, C/05.7  **ПС 06.033**  ОТФ С  ТФ C/03.6  **ПС 06.006**  ОТФ A  ТФ A/02.6  ОТФ B  ТФ B/02.6  ОТФ C  ТФ C/02.6, C/03.6 |
| ОПК-13.1.2 | знает основные системы и сети электрической связи, включая локальные и глобальные сети, сеть «интернета вещей», принципы их построения и технические характеристики входящих в них элементов |
| ОПК-13.2.1 | умеет оценивать технические возможности основных систем и сетей электрической связи |
| ОПК-13.1.3 | знает основные уязвимости элементов информационно-телекоммуникационной инфраструктуры и принципы обеспечения её информационной безопасности | Комплексное обеспечение защиты информации телекоммуникационных систем |
| ОПК-13.1.4 | знает основные угрозы безопасности информации и модели нарушителя, принципы формирования политики информационной безопасности телекоммуникационной системы |
| ОПК-13.2.2 | умеет анализировать угрозы информационно-телекоммуникационной инфраструктуре и циркулирующей в ней информации, выбирать необходимые средства для обеспечения информационной безопасности |
| ОПК-13.3.1 | владеет навыком оценки технических возможностей и подготовки рекомендаций по построению отдельных элементов информационно-телекоммуникационной инфраструктуры с учетом обеспечения требований информационной безопасности | Производственная (преддипломная) практика |
| **ОПК-14. Способен применять технологии и технические средства сетей электросвязи** | ОПК-14.1.1 | знает элементную базу телекоммуникационных систем, включая области применения и основные характеристики, принципы организации систем на кристалле | Аппаратные средства телекоммуникационных систем | **ПС 06.030**  ОТФ A  ТФ A/01.5, A/02.5, A/03.5  ОТФ D  ТФ D/02.7  **ПС 06.034**  ОТФ B  ТФ B/01.6  **ПС 06.027**  ОТФ A  ТФ A/01.4, A/03.4  ОТФ B  ТФ B/01.5  ОТФ E  ТФ E/01.6, E/03.6  ОТФ F  ТФ F/01.7, F/03.7  **ПС 06.023**  ОТФ C  ТФ C/02.3  **ПС 06.006**  ОТФ A  ТФ A/01.6  ОТФ B  ТФ B/01.6  ОТФ C  ТФ C/01.6  **ПС 06.018**  ОТФ A  ТФ A/02.6  ОТФ B  ТФ B/02.6, B/03.6 |
| ОПК-14.1.2 | знает основные архитектуры аппаратных средств телекоммуникационных систем и их отличия |
| ОПК-14.1.3 | знает технологии аппаратной обработки «больших данных», построения распределённых систем и систем искусственного интеллекта |
| ОПК-14.2.1 | умеет выбирать технологии и аппаратные средства телекоммуникационных систем и реализовывать на их основе отдельные узлы и устройства |
| ОПК-14.1.4 | знает состав и основные характеристики технических средств сетей электросвязи | Сети и системы передачи информации |
| ОПК-14.2.2 | умеет эксплуатировать и настраивать типовые технические средства сетей электросвязи, проводить диагностику типовых неисправностей в работе средств связи сетей электросвязи и исправлять их |
| **ОПК-15. Способен проводить инструментальный мониторинг качества обслуживания и анализ защищенности информации от несанкционированного доступа в телекоммуникационных системах и сетях в целях управления их функционированием** | ОПК-15.1.1 | знает методики измерения и оценки параметров в телекоммуникационных системах и сетях | Измерения в телекоммуникационных системах | **ПС 06.030**  ОТФ B  ТФ B/01.6  **ПС 06.032**  ОТФ C  ТФ C/05.7  **ПС 06.033**  ОТФ B  ТФ B/03.6, B/05.6, B/06.6  **ПС 06.027**  ОТФ B  ТФ B/03.5  ОТФ D  ТФ D/01.6  **ПС 06.018**  ОТФ A  ТФ A/02.6, A/03.6  ОТФ B  ТФ B/01.6, B/04.6 |
| ОПК-15.2.1 | умеет анализировать пропускную способность и предельную нагрузку сети связи, параметры передачи кадров при прохождении по каналам связи, проверять достижимость абонентов сети связи |
| ОПК-15.1.2 | знает типовые средства для инструментальной оценки уровня защищённости телекоммуникационных систем | Комплексное обеспечение защиты информации телекоммуникационных систем |
| ОПК-15.2.2 | умеет проводить анализ защищенности информации от несанкционированного доступа в телекоммуникационных системах и сетях |
| **ОПК-16. Способен проектировать защищенные телекоммуникационные системы и их элементы, проводить анализ проектных решений по обеспечению заданного уровня безопасности и требуемого качества обслуживания телекоммуникационных систем, разрабатывать необходимую техническую документацию с учетом действующих нормативных и методических документов, проводить подготовку исходных данных для технико-экономического обоснования соответствующих проектных решений** | ОПК-16.1.1 | знает общие принципы проектирования систем и сетей электрической связи и принципы построения защищенных телекоммуникационных систем | Проектирование защищенных телекоммуникационных систем | **ПС 06.030**  ОТФ D  ТФ D/02.7  **ПС 06.033**  ОТФ C  ТФ C/03.6  ОТФ D  ТФ D/02.6, D/03.6  **ПС 06.007**  ОТФ B  ТФ B/01.6, B/02.6, B/04.6, B/06.6, B/07.6  **ПС 06.006**  ОТФ A  ТФ A/02.6  ОТФ B  ТФ B/02.6  ОТФ C  ТФ C/02.6, C/03.6  **ПС 06.018**  ОТФ C  ТФ C/02.7  ОТФ D  ТФ D/01.7, D/02.7, D/03.7 |
| ОПК-16.1.2 | знает номенклатуру и содержание нормативных правовых актов и нормативных методических документов, применяемых при проектировании защищенных телекоммуникационных систем |
| ОПК-16.1.3 | знает состав технико-экономического обоснования проектируемых защищенных телекоммуникационных систем |
| ОПК-16.2.1 | умеет разрабатывать необходимую техническую документацию в области проектирования защищенных телекоммуникационные систем с учетом действующих нормативных и методических документов |
| ОПК-16.2.2 | умеет проводить подготовку исходных данных для технико-экономического обоснования проектируемых защищенных телекоммуникационных систем |
| ОПК-16.2.3 | умеет анализировать проектные решения по обеспечению заданного уровня безопасности и требуемого качества обслуживания телекоммуникационных систем | Производственная (преддипломная) практика |
| ОПК-16.2.4 | умеет проектировать элементы защищенных телекоммуникационных систем |
| **ОПК-17. Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма** | ОПК-17.1.1 | знает периодизацию, основные факты, явления и процессы всемирной и отечественной истории | Дисциплина (модуль) по истории (истории России, всеобщей истории) |  |
| ОПК-17.1.2 | знает особенности исторического пути России, ее место и роль в мировом сообществе в контексте всеобщей истории |
| ОПК-17.2.1 | умеет анализировать основные этапы и закономерности исторического развития России, в том числе для формирования гражданской позиции и развития патриотизма |
| **специализация № 6 «Информационная безопасность аэрокосмических телекоммуникационных систем»** | | | | |
| **ОПК-6.1. Способен выбирать методы и разрабатывать средства защиты объектов аэрокосмических телекоммуникационных систем при воздействии радиопомех** | ОПК-6.1.1.1 | знает принципы построения и функционирования космических комплексов координатно-временного обеспечения | Телекоммуникационные системы комплексов координатно-временного обеспечения | **ПС 06.030**  ОТФ D  ТФ D/02.7 |
| ОПК-6.1.1.2 | знает основные методы и средства защиты комплексов координатно-временного обеспечения |
| ОПК-6.1.2.1 | умеет проектировать защищенные телекоммуникационные системы в условиях воздействия радиопомех со стороны злоумышленника, низкого отношения сигнал/шум и влияния эффекта Доплера |
| ОПК-6.1.1.3 | знает принципы построения и функционирования телеметрических систем | Проектирование защищенных телекоммуникационных систем в контуре управления космическим аппаратом |
| ОПК-6.1.1.4 | знает принципы построения и функционирования командных систем |
| ОПК-6.1.1.5 | знает основные принципы и классы управления космическими объектами |
| ОПК-6.1.2.2 | умеет проектировать защищенные телеметрические системы |
| ОПК-6.1.2.3 | умеет проектировать защищенные командные системы |
| **ОПК-6.2. Способен проектировать системы защищенного информационного взаимодействия объектов аэрокосмического и наземного сегментов** | ОПК-6.2.1.1 | знает защищенные протоколы управления объектами аэрокосмического сегмента телекоммуникационной системы | Протоколы сетевого взаимодействия объектов аэрокосмического и наземного сегментов телекоммуникационной системы | **ПС 06.030**  ОТФ D  ТФ D/02.7  **ПС 06.027**  ОТФ D  ТФ D/03.6 |
| ОПК-6.2.1.2 | знает сетевые протоколы информационного взаимодействия аэрокосмического и наземного сегментов и параметры их настройки |
| ОПК-6.2.1.3 | знает топологии и протоколы сетевого взаимодействия, применяемые в эксплуатируемых сетях наземного сегмента аэрокосмической телекоммуникационной системы |
| ОПК-6.2.2.1 | умеет устанавливать и настраивать параметры сетевых протоколов, реализованных в телекоммуникационном оборудовании объектов аэрокосмического и наземного сегментов |
| ОПК-6.2.2.2 | умеет наблюдать и оценивать информационные потоки на объектах аэрокосмического и наземного сегментов с помощью пакетных анализаторов |
| ОПК-6.2.3.1 | владеет основными приемами борьбы с уязвимостями реализаций протоколов сетевого взаимодействия, применяемых в эксплуатируемых сетях наземного сегмента аэрокосмической телекоммуникационной системы |
| ОПК-6.2.1.4 | знает типовые сетевые атаки и способы защиты от них | Защита информационных процессов в телекоммуникационных сетях обеспечения функционирования летательных аппаратов |
| ОПК-6.2.1.5 | знает методы и средства контроля уровня безопасности информационных процессов в сетях обработки данных с летательных аппаратов |
| ОПК-6.2.2.3 | умеет применять программно-аппаратные средства защиты объектов аэрокосмического и наземного сегментов телекоммуникационной системы от несанкционированного доступа |
| ОПК-6.2.2.4 | умеет применять методы задания базовых параметров и параметров защиты от несанкционированного доступа к операционным системам объектов наземного сегмента аэрокосмических телекоммуникационных систем |
| **ОПК-6.3. Способен разрабатывать инфокоммуникационные системы, энергетически эффективно и скрытно использующие радиоканал для информационного взаимодействия** | ОПК-6.3.1.1 | знает назначение, типы и основные характеристики радиолиний аэрокосмических систем | Методы защиты радиолиний аэрокосмических телекоммуникационных систем с использованием перспективных сигнально-кодовых конструкций | **ПС 06.030**  ОТФ D  ТФ D/02.7 |
| ОПК-6.3.1.2 | знает методы и средства повышения скрытности использования радиолиний аэрокосмических систем |
| ОПК-6.3.1.3 | знает основные уязвимости радиоканалов аэрокосмических телекоммуникационных систем и методы их защиты |
| ОПК-6.3.2.1 | умеет формировать исходные данные и ограничения при проектировании аэрокосмических телекоммуникационных систем и сетей |
| ОПК-6.3.2.2 | умеет разрабатывать энергетически эффективные инфокоммуникационные системы со скрытыми радиоканалами информационного взаимодействия |
| ОПК-6.3.3.1 | владеет приемами и методикой выполнения спектрального анализа сигнально-кодовых конструкций для обеспечения энергетической и структурной скрытности в радиоканалах беспилотных летательных аппаратов |
| **специализация № 7 «Разработка защищенных телекоммуникационных систем»** | | | | |
| **ОПК-7.1. Способен формировать техническое задание и разрабатывать аппаратное и программное обеспечение компонентов защищенных телекоммуникационных систем** | ОПК-7.1.1.1 | знает современную элементную базу компонентов защищенных телекоммуникационных систем | Разработка аппаратного и программного обеспечения узлов и устройств защищенных телекоммуникационных систем | **ПС 06.030**  ОТФ D  ТФ D/02.7  **ПС 06.033**  ОТФ D  ТФ D/02.7, D/04.7 |
| ОПК-7.1.1.2 | знает средства проектирования цифровых узлов и устройств защищенных телекоммуникационных систем на базе ПЛИС |
| ОПК-7.1.1.3 | знает функциональные возможности ПЛИС при разработке аппаратного и программного обеспечения типовых узлов и устройств защищенных телекоммуникационных систем |
| ОПК-7.1.2.1 | умеет проводить анализ компонентов защищенных телекоммуникационных систем на базе ПЛИС |
| ОПК-7.1.2.2 | умеет выбирать архитектуры ПЛИС при разработке типовых узлов и устройств защищенных телекоммуникационных систем |
| ОПК-7.1.2.3 | умеет учитывать требования информационной безопасности при разработке технического задания на аппаратное и программное обеспечение компонентов защищенных телекоммуникационных систем. |
| ОПК-7.1.3.1 | владеет навыками работы с инструментальными средствами разработки узлов и устройств защищенных телекоммуникационных систем на базе ПЛИС |
| **ОПК-7.2. Способен участвовать в разработке систем управления информационной безопасностью телекоммуникационных систем** | ОПК-7.2.1.1 | знает процессы и методы планирования системы управления информационной безопасностью телекоммуникационных систем | Управление информационной безопасностью телекоммуникационных систем | **ПС 06.030**  ОТФ B  ТФ B/02.7  ОТФ D  ТФ D/02.7  **ПС 06.033**  ОТФ B  ТФ B/03.7 |
| ОПК-7.2.1.2 | знает основные методы идентификации, анализа, оценивания и обработки рисков |
| ОПК-7.2.1.3 | знает процессы и методы поддержки и функционирования системы управления информационной безопасностью телекоммуникационных систем |
| ОПК-7.2.1.4 | знает процессы и методы проверки функционирования и совершенствования системы управления информационной безопасностью телекоммуникационных систем |
| ОПК-7.2.2.1 | умеет определять и обосновывать активы, ресурсы, роли для процессов системы управления информационной безопасностью телекоммуникационных систем |
| ОПК-7.2.2.2 | умеет определять возможность применения соответствующего математического аппарата при использовании количественных и качественных методов оценки рисков |
| ОПК-7.2.3.1 | владеет навыками формирования и описания процессов системы управления информационной безопасностью телекоммуникационных систем |
| **ОПК-7.3. Способен обеспечивать защиту программных средств защищенных телекоммуникационных систем** | ОПК-7.3.1.1 | знает принципы работы инструментальных средств исследования программного обеспечения защищенных телекоммуникационных систем | Защита программных средств защищенных телекоммуникационных систем | **ПС 06.030**  ОТФ D  ТФ D/01.7, D/02.7  **ПС 06.032**  ОТФ C  ТФ C/03.7, D/05.7 |
| ОПК-7.3.1.2 | знает принципы и средства защиты программного обеспечения защищенных телекоммуникационных систем |
| ОПК-7.3.2.1 | умеет выявлять уязвимости защиты программных средств защищенных телекоммуникационных систем и находить пути их устранения |
| ОПК-7.3.2.2 | умеет проектировать и реализовывать защиту программных средств защищенных телекоммуникационных систем, исходя из поставленных целей защиты |
| ОПК-7.3.3.1 | владеет навыками работы с инструментальными средствами для исследования программных средств защищенных телекоммуникационных систем |
| **специализация № 8 «Защита информации в радиосвязи и телерадиовещании»** | | | | |
| **ОПК-8.1. Способен осуществлять частотно-территориальное и кодовое планирование сетей радиосвязи и телерадиовещания** | ОПК-8.1.1.1 | знает теоретические основы частотно-временного и кодового планирования сетей радиосвязи и телерадиовещания | Системы радиосвязи и сети телерадиовещания | **ПС 06.030**  ОТФ B  ТФ B/02.6  **ПС 06.018**  ОТФ D  ТФ D/02.7, D/03.7 |
| ОПК-8.1.1.2 | знает принципы и методы частотного планирования сетей телерадиовещания |
| ОПК-8.1.2.1 | умеет выбирать методы частотно-временного и кодового планирования сетей радиосвязи и телерадиовещания |
| ОПК-8.1.2.2 | умеет применять технологии частотно-временного и кодового планирования для разработки сетей радиосвязи и телерадиовещания |
| ОПК-8.1.3.1 | владеет инструментарием решения вопросов выделения частот каналов для развития сетей радиосвязи и телерадиовещания |
| **ОПК-8.2. Способен применять методы приема, передачи и обработки сигналов, обеспечивающие повышение эффективности и защищенности систем радиосвязи и телерадиовещания** | ОПК-8.2.1.1 | знает теоретические основы приема, передачи и обработки сигналов в целях обеспечения эффективности и защищенности систем радиосвязи и телерадиовещания | Устройства приема и обработки сигналов в защищенных системах радиосвязи | **ПС 06.030**  ОТФ D  ТФ D/02.7 |
| ОПК-8.2.1.2 | знает основные понятия и принципы защиты информации в системах радиосвязи и телерадиовещания |
| ОПК-8.2.2.1 | умеет использовать методы повышения помехозащищенности систем телерадиовещания |
| ОПК-8.2.2.2 | умеет анализировать системы радиосвязи на предмет защищенности |
| ОПК-8.2.3.1 | владеет навыками решения типовых задач повышения эффективности и защищенности систем радиосвязи и телерадиовещания |
| **ОПК-8.3. Способен разрабатывать системы, сети и устройства защищенной радиосвязи и телерадиовещания** | ОПК-8.3.1.1 | знает принципы и стандарты построения систем, сетей и устройств защищенной радиосвязи и телерадиовещания | Защита информации в системах радиосвязи и телерадиовещания | **ПС 06.030**  ОТФ D  ТФ D/02.7 |
| ОПК-8.3.1.2 | знает технологии создания систем, сетей и устройств защищенной радиосвязи и телерадиовещания |
| ОПК-8.3.2.1 | умеет разрабатывать системы, сети и устройств защищенной радиосвязи и телерадиовещания |
| ОПК-8.3.2.2 | умеет решать типовые задачи по проектированию защищенных сетей радиосвязи и телерадиовещания |
| ОПК-8.3.3.1 | владеет базовыми навыками решения типовых задач создания систем, сетей и устройств защищенной радиосвязи и телерадиовещания |
| **специализация № 9 «Управление безопасностью телекоммуникационных систем и сетей»** | | | | |
| **ОПК-9.1. Способен формировать, внедрять и обеспечивать функционирование системы менеджмента информационной безопасности телекоммуникационных систем и сетей** | ОПК-9.1.1.1 | знать основные методы управления информационной безопасностью телекоммуникационных систем и сетей | Менеджмент информационной безопасности телекоммуникационных систем и сетей | **ПС 06.030**  ОТФ В  ТФ В/02.6, В/03.6  ОТФ F  ТФ F/01.7  **ПС 06.032**  ОТФ С  ТФ С/02.7, С/03.7 |
| ОПК-9.1.1.2 | знать методику выработки и реализации управленческих решений по обеспечению защиты телекоммуникационных систем и сетей |
| ОПК-9.1.1.3 | знать цели и задачи управления персоналом по обеспечению защиты телекоммуникационных систем и сетей |
| ОПК-9.1.2.1 | уметь определять угрозы, реализация которых может привести к нарушению безопасности и корректности функционирования телекоммуникационных систем и сетей |
| ОПК-9.1.2.2 | уметь разрабатывать политику безопасности телекоммуникационных систем и сетей |
| ОПК-9.1.2.3 | уметь производить постановку задач персоналу по обеспечению защиты телекоммуникационных систем и сетей |
| ОПК-9.1.3.1 | владеть навыками оценки рисков, связанных с осуществлением угроз безопасности телекоммуникационных систем и сетей |
| **ОПК-9.2. Способен реализовывать комплекс организационных мероприятий по обеспечению информационной безопасности и устойчивости телекоммуникационных систем и сетей** | ОПК-9.2.1.1 | знать содержание и порядок деятельности персонала при вводе в эксплуатацию (выводе из эксплуатации) телекоммуникационных систем и сетей | Правила и процедуры по обеспечению информационной безопасности телекоммуникационных систем и сетей | **ПС 06.030**  ОТФ A  ТФ A/02.5, A/03.5  ОТФ В  ТФ В/03.6  **ПС 06.033**  ОТФ С  ТФ С/02.6, С/04.6 |
| ОПК-9.2.1.2 | знать содержание и порядок деятельности персонала при эксплуатации телекоммуникационных систем и сетей |
| ОПК-9.2.1.3 | знать содержание и порядок деятельности персонала по выявлению и реагированию на инциденты информационной безопасности |
| ОПК-9.2.2.1 | уметь определять правила и процедуры защиты информации при вводе в эксплуатацию (выводе из эксплуатации) телекоммуникационных систем и сетей |
| ОПК-9.2.2.2 | уметь определять правила и процедуры защиты информации при эксплуатации телекоммуникационных систем и сетей |
| ОПК-9.2.2.3 | уметь определять правила и процедуры выявления и реагирования на инциденты информационной безопасности |
| ОПК-9.2.1.4 | знать типы, основные характеристики средств измерений и контроля процесса и параметров функционирования телекоммуникационных систем и сетей | Обеспечение устойчивости телекоммуникационных систем и сетей |
| ОПК-9.2.1.5 | знать способы организации, методики, нормативные требования и содержание технического обслуживания телекоммуникационных систем и сетей |
| ОПК-9.2.1.6 | знать методики и нормативные требования к действиям в целях восстановления процесса и параметров функционирования телекоммуникационных систем и сетей |
| ОПК-9.2.2.3 | уметь проводить текущий контроль показателей и процесса функционирования телекоммуникационных систем и сетей, предусмотренный регламентом их эксплуатации |
| ОПК-9.2.2.4 | уметь проводить предусмотренные регламентом работы по восстановлению процесса и параметров функционирования телекоммуникационных систем и сетей |
| ОПК-9.2.3.1 | владеть навыками восстановления процесса функционирования после сбоев и отказов телекоммуникационных систем и сетей |
| **ОПК-9.3. Способен проводить мониторинг защищенности сетевых ресурсов и формировать отчеты по выявленным уязвимостям** | ОПК-9.3.1.1 | знать методы контроля функционирования телекоммуникационных систем и сетей | Мониторинг безопасности телекоммуникационных систем и сетей | **ПС 06.030**  ОТФ В  ТФ В/01.6  **ПС 06.032**  ОТФ C  ТФ C/05.7  **ПС 06.033**  ОТФ B  ТФ B/05.6 |
| ОПК-9.3.1.2 | знать принципы построения систем обнаружения компьютерных атак |
| ОПК-9.3.1.3 | знать методы обработки данных мониторинга безопасности телекоммуникационных систем и сетей |
| ОПК-9.3.2.1 | уметь применять средства мониторинга работоспособности и эффективности применяемых средств защиты телекоммуникационных систем и сетей |
| ОПК-9.3.2.2 | уметь применять инструментальные средства проведения мониторинга защищенности сетевых ресурсов телекоммуникационных систем и сетей |
| ОПК-9.3.2.3 | уметь составлять отчеты по результатам проверок защищенности телекоммуникационных систем и сетей |
| ОПК-9.3.3.1 | владеть навыками анализа защищенности телекоммуникационных систем и сетей с использованием сканеров безопасности и средств автоматического реагирования на попытки несанкционированного доступа |
| **специализация № 10 «Информационная безопасность мультисервисных телекоммуникационных сетей и систем на транспорте» (по видам)** | | | | |
| **ОПК-10.1. Способен проводить теоретические и экспериментальные исследования телекоммуникационных систем и сетей транспорта (по видам) и оценивать их эффективность** | ОПК-10.1.1.1. | знает основные принципы квантовых вычислений и квантовой связи, используемые в задачах криптографии | Квантовая криптография в телекоммуникационных системах и сетях транспорта | **ПС 06.030**  ОТФ D  ТФ D/03.7 |
| ОПК-10.1.1.2 | знает квантовые коммуникации (квантовое распределение ключей) |
| ОПК-10.1.1.3 | знает принципы квантово-криптографической защиты высокоскоростных оптических линий связи |
| ОПК-10.1.1.4 | знает постквантовые алгоритмы и принципы оптических измерений в телекоммуникационных системах и сетях транспорта |
| ОПК-10.1.2.1 | умеет формулировать предложения по вопросам обеспечения информационной безопасности с использованием квантовой криптографии в телекоммуникационных системах на транспорте |
| ОПК-10.1.2.2 | умеет проводить исследование уязвимостей и разрабатывать модели оценки телекоммуникационных систем, построенных на технологиях квантовой криптографии и квантовых сетей |
| ОПК-10.1.3.1 | владеет методиками расчета и оценки эффективности защиты с использованием квантовой криптографии в телекоммуникационных систем и сетях на транспорте. |
| **ОПК-10.2. Способен осуществлять рациональный выбор методов и средств обеспечения информационной безопасности мультисервисных телекоммуникационных систем и сетей транспорта (по видам)** | ОПК-10.2.1.1 | знает информационную структуру сетей транспорта как объекта защиты | Информационная безопасность и защита информации в интегрированных телекоммуникационных и корпоративных сетях транспорта | **ПС 06.030**  ОТФ A  ТФ A/01.5, A/02.5, A/03.5 |
| ОПК-10.2.1.2 | знает информационные ресурсы сетей транспорта как объекта защиты |
| ОПК-10.2.1.3 | знает критерии оценки защищенности телекоммуникационных систем и систем транспорта |
| ОПК-10.2.2.1 | умеет использовать программно-аппаратные методы защиты информации телекоммуникационных систем и сетей транспорта |
| ОПК-10.2.2.2 | умеет использовать криптографические методы защиты информации телекоммуникационных систем и сетей транспорта |
| ОПК-10.2.3.1 | владеет навыками работы с программно-аппаратными средствами обеспечения информационной безопасности телекоммуникационных систем и сетей транспорта |
| **ОПК-10.3. Способен использовать методы и средства измерений для решения метрологических задач и технической диагностики защищенных телекоммуникационных систем и сетей транспорта (по видам)** | ОПК-10.3.1.1 | знает структуру и характеристики средств технического диагностирования и контроля, используемых в защищенных системах и сетях транспорта | Специальные измерения и техническая диагностика в защищенных сетях транспорта | **ПС 06.030**  ОТФ D  ТФ D/01.7 |
| ОПК-10.3.1.2 | знает основные технические характеристикиконтрольно-измерительных приборов параметров телекоммуникационных систем и сетей транспорта |
| ОПК-10.3.1.3 | знает основные положения национальных, межгосударственных и международных стандартов в части телекоммуникационных систем и сетей транспорта |
| ОПК-10.3.2.1 | умеет использовать и приборы общего и специального назначения для оценки функционального состояния телекоммуникационных систем и сетей транспорта; |
| ОПК-10.3.2.2 | умеет осуществлять выбор совокупности параметров для определения работоспособности защищенной телекоммуникационной системы транспорта |
| ОПК-10.3.2.3 | умеет осуществлять оценку технических возможностей систем и сетей передачи информации при аттестации телекоммуникационных систем транспорта учётом требований по защите информации |
| ОПК-10.3.3.1 | владеет методами прогнозирования технического состояния средств защиты информации телекоммуникационных систем и защищенной телекоммуникационной системы транспорта |
| ОПК-10.3.3.2 | владеет навыками работы со средствами и системами тестирования телекоммуникационных систем на транспорте (по видам транспорта) |
| **специализация № 11 «Системы подвижной цифровой защищенной связи»** | | | | |
| **ОПК-11.1. Способен выбирать методы, разрабатывать и реализовывать алгоритмы для обеспечения безопасности систем подвижной цифровой защищенной связи** | ОПК-11.1.1.1 | знает методы и алгоритмы обеспечения безопасности систем подвижной цифровой защищенной связи | Основы цифровых телекоммуникационных сетей | **ПС 06.030**  ОТФ D  ТФ D/02.7  **ПС 06.007**  ОТФ B  ТФ B/06.6, B/07.6 |
| ОПК-11.1.2.1 | умеет выбирать методы и разрабатывать алгоритмы обеспечения безопасности систем подвижной цифровой защищенной связи |
| ОПК-11.1.3.1 | владеет базовыми навыками реализации алгоритмов обеспечения безопасности систем подвижной цифровой защищенной связи |
| ОПК-11.1.1.2 | знает характеристики беспроводных каналов связи и методы их расчета | Свойства беспроводных каналов связи |
| ОПК-11.1.2.2 | умеет рассчитывать основные характеристики беспроводных каналов связи |
| **ОПК-11.2. Способен контролировать работоспособность и оценивать эффективность средств защиты информации в системах подвижной цифровой защищенной связи** | ОПК-11.2.1.1 | знает аппаратное и программное обеспечение узлов и устройств систем подвижной цифровой защищенной связи | Беспроводные системы связи и их безопасность | **ПС 06.030**  ОТФ B  ТФ B/01.6  ОТФ D  ТФ D/01.7 |
| ОПК-11.2.1.2 | знает методы контроля работоспособности и оценки эффективности программно-аппаратных средств защиты информации в системах подвижной цифровой защищенной связи |
| ОПК-11.2.2.1 | умеет оценивать эффективность программно-аппаратных средств защиты информации в системах подвижной цифровой защищенной связи |
| ОПК-11.2.3.1 | владеет навыками контроля работоспособности программно-аппаратных средств защиты информации в системах подвижной цифровой защищенной связи |
| ОПК-11.2.1.3 | знает основные подходы к построению математических моделей криптосистем и их функциональных элементов как динамических объектов | Алгоритмы идентификации динамических моделей криптосистем |
| ОПК-11.2.2.2 | умеет определять базовые параметры математических моделей криптосистем |
| ОПК-11.2.2.3 | умеет оценивать параметры криптографической стойкости шифров на основе базовых параметров их экспериментальных данных |
| **ОПК-11.3. Способен использовать и реализовывать алгоритмы распределенной обработки информации и сигналов в целях обеспечения безопасности систем подвижной цифровой защищенной связи** | ОПК-11.3.1.1 | знает принципы построения и функционирования наземных радионавигационных систем дальнего и ближнего действия, обеспечивающих безопасную работу систем подвижной цифровой защищенной связи | Системы позиционирования подвижных объектов | **ПС 06.030**  ОТФ D  ТФ D/02.7 |
| ОПК-11.3.1.2 | знает принципы построения и функционирования спутниковых радионавигационных систем, обеспечивающих безопасную работу систем подвижной цифровой защищенной связи |
| ОПК-11.3.2.1 | умеет реализовывать методы и алгоритмы измерения навигационных параметров, применяемые в радионавигационных системах |
| ОПК-11.3.2.2 | умеет реализовывать методы и алгоритмы определения местоположения подвижного объекта |
| ОПК-11.3.1.3 | знает способы разнесенного приема сигналов | Свойства беспроводных каналов связи |
| ОПК-11.3.2.3 | умеет использовать разнесенный прием сигналов для повышения безопасности систем подвижной цифровой защищенной связи |
| **специализация № 12 «Техническая защита информации информационно-телекоммуникационных систем»** | | | | |
| **ОПК-12.1. Способен проектировать системы технической защиты информации для объектов информатизации** | ОПК-12.1.1.1 | знает технические каналы утечки информации, обрабатываемой средствами вычислительной техники, возможности специальных технических средств по перехвату информации, обрабатываемой средствами вычислительной техники | Защита информации от утечки по техническим каналам. Дополнительные главы | **ПС 06.033**  ОТФ D  ТФ D/02.7  **ПС 06.034**  ОТФ F  ТФ F/02.7 |
| ОПК-12.1.1.2 | знает технические каналы утечки акустической речевой информации, возможности средств акустической речевой разведки по перехвату разговоров из выделенных помещений |
| ОПК-12.1.1.3 | знает принципы построения и основные характеристики средств защиты объектов информатизации от утечки информации по техническим каналам |
| ОПК-12.1.1.4 | знает принципы построения и основные характеристики средств защиты выделенных помещений от утечки речевой информации по техническим каналам |
| ОПК-12.1.1.5 | знает организацию защиты объектов информатизации от утечки информации по техническим каналам |
| ОПК-12.1.2.1 | умеет проводить анализ потенциальных технических каналов утечки информации на объектах информатизации и речевой информации в выделенных помещениях |
| ОПК-12.1.2.2 | умеет обосновывать требования к подсистеме защиты объекта информатизации от утечки информации по техническим каналам |
| ОПК-12.1.1.6 | знает методы и средства контроля защищенности информации от утечки по техническим каналам | Аттестация объектов информатизации |
| ОПК-12.1.1.7 | знает основные классы и виды уязвимостей программного обеспечения, угрозы несанкционированного доступа к информации и специальных программных воздействий на информацию и ее носители в автоматизированных системах | Программно-аппаратные средства защиты информации. Дополнительные главы |
| ОПК-12.1.1.8 | знает способы и средства защиты информации, обрабатываемой автоматизированными системами, от несанкционированного доступа и специальных программных воздействий на нее |
| ОПК-12.1.1.9 | знает методы и средства контроля защищенности информации, обрабатываемой автоматизированными системами, от несанкционированного доступа и специальных программных воздействий на нее |
| ОПК-12.1.2.3 | умеет применять технологии защиты информации от несанкционированного доступа для обеспечения безопасности автоматизированных систем и вычислительных сетей |
| ОПК-12.1.1.10 | знает нормативные правовые акты, методические документы, национальные стандарты в области проектирования систем защиты информации объектов информатизации | Проектирование систем защиты объектов информатизации |
| ОПК-12.1.1.11 | знает порядок создания автоматизированных систем в защищенном исполнении |
| ОПК-12.1.2.4 | умеет проводить анализ угроз безопасности информации на объекте информатизации |
| ОПК-12.1.2.5 | умеет проводить предпроектное обследование объекта информатизации |
| ОПК-12.1.2.6 | умеет разрабатывать аналитическое обоснование необходимости создания системы защиты информации объекта информатизации |
| ОПК-12.1.2.7 | умеет разрабатывать техническое задание на создание системы защиты информации объекта информатизации |
| ОПК-12.1.2.8 | умеет разрабатывать технический проект системы защиты информации объекта информатизации |
| ОПК-12.1.2.9 | умеет разрабатывать эксплуатационную документацию на системы защиты информации, организационно-распорядительную документацию по защите информации на объекте информатизации |
| **ОПК-12.2 Способен проектировать средства и системы информатизации в защищенном исполнении** | ОПК-12.2.1.1 | знает технические каналы утечки информации, обрабатываемой средствами вычислительной техники, возможности специальных технических средств по перехвату информации, обрабатываемой средствами вычислительной техники | Защита информации от утечки по техническим каналам. Дополнительные главы | **ПС 06.033**  ОТФ D  ТФ D/02.7  **ПС 06.034**  ОТФ F  ТФ F/01.7 |
| ОПК-12.2.1.2 | знает технические каналы утечки акустической речевой информации, возможности средств акустической речевой разведки по перехвату разговоров из выделенных помещений |
| ОПК-12.2.1.3 | знает принципы построения и основные характеристики средств защиты объектов информатизации от утечки информации по техническим каналам |
| ОПК-12.2.1.4 | знает принципы построения и основные характеристики средств защиты выделенных помещений от утечки речевой информации по техническим каналам |
| ОПК-12.2.1.5 | знает методы и средства контроля защищенности информации от утечки по техническим каналам | Аттестация объектов информатизации |
| ОПК-12.2.1.6 | знает основные классы и виды уязвимостей программного обеспечения, угрозы несанкционированного доступа к информации и специальных программных воздействий на информацию и ее носители в автоматизированных системах | Программно-аппаратные средства защиты информации. Дополнительные главы |
| ОПК-12.2.1.7 | знает способы и средства защиты информации, обрабатываемой автоматизированными системами, от несанкционированного доступа и специальных программных воздействий на нее |
| ОПК-12.2.1.8 | знает методы и средства контроля защищенности информации, обрабатываемой автоматизированными системами, от несанкционированного доступа и специальных программных воздействий на нее |
| ОПК-12.2.1.9 | знает нормативные правовые акты, методические документы, национальные стандарты в области проектирования средств и систем информатизации в защищенном исполнении | Проектирование систем защиты объектов информатизации |
| ОПК-12.2.1.10 | знает порядок создания автоматизированных систем в защищенном исполнении |
| ОПК-12.2.1.11 | знает виды испытаний технических средств обработки информации в защищенном исполнении и общие требования к их проведению |
| ОПК-12.2.2.1 | умеет формировать требования к средствам и системам информатизации в защищенном исполнении |
| ОПК-12.2.2.2 | умеет разрабатывать концепцию средств и систем информатизации в защищенном исполнении |
| ОПК-12.2.2.3 | умеет разрабатывать техническое задание на создание средства и/или системы информатизации в защищенном исполнении |
| ОПК-12.2.2.4 | умеет разрабатывать технический проект средства и/или системы информатизации в защищенном исполнении |
| ОПК-12.2.2.5 | умеет разрабатывать программы и методики испытаний средства и/или системы информатизации в защищенном исполнении |
| ОПК-12.2.2.6 | умеет разрабатывать рабочую и эксплуатационную документацию на средства и системы информатизации в защищенном исполнении |
| **ОПК-12.3. Способен проводить аттестацию объектов информатизации на соответствие требованиям по защите информации** | ОПК-12.3.1.1 | знает технические каналы утечки информации, обрабатываемой средствами вычислительной техники, возможности специальных технических средств по перехвату информации, обрабатываемой средствами вычислительной техники | Защита информации от утечки по техническим каналам. Дополнительные главы | **ПС 06.034**  ОТФ G  ТФ G/01.7 |
| ОПК-12.3.1.2 | знает технические каналы утечки акустической речевой информации, возможности средств акустической речевой разведки по перехвату разговоров из выделенных помещений |
| ОПК-12.3.2.1 | умеет проводить анализ потенциальных технических каналов утечки информации на объектах информатизации и речевой информации в выделенных помещениях |
| ОПК-12.3.1.3 | знает основные классы и виды уязвимостей программного обеспечения, угрозы несанкционированного доступа к информации и специальных программных воздействий на информацию и ее носители в автоматизированных системах | Программно-аппаратные средства защиты информации. Дополнительные главы |
| ОПК-12.3.1.4 | знает способы и средства защиты информации, обрабатываемой автоматизированными системами, от несанкционированного доступа и специальных программных воздействий на нее |
| ОПК-12.3.1.5 | знает методы и средства контроля защищенности информации, обрабатываемой автоматизированными системами, от несанкционированного доступа и специальных программных воздействий на нее |
| ОПК-12.3.2.2 | умеет проводить контроль защищенности информации, обрабатываемой автоматизированными системами, от несанкционированного доступа |
| ОПК-12.3.1.6 | знает нормативные правовые акты, методические документы, национальные стандарты в области аттестации объектов информатизации | Аттестация объектов информатизации |
| ОПК-12.3.1.7 | знает методы, средства и методики контроля защищенности информации от утечки по техническим каналам |
| ОПК-12.3.1.8 | знает порядок проведения аттестации объектов информатизации на соответствие требованиям по защите информации |
| ОПК-12.3.1.9 | знает отчетные документы, оформляемые по результатам аттестации объектов вычислительной техники на соответствие требованиям по защите информации |
| ОПК-12.3.2.3 | умеет разрабатывать программы и методики аттестационных испытаний объектов вычислительной техники на соответствие требованиям по защите информации |
| ОПК-12.3.2.4 | умеет проводить аттестационные испытания объектов вычислительной техники на соответствие требованиям по защите информации |
| ОПК-12.3.2.5 | умеет оформлять материалы аттестационных испытаний (протоколы аттестационных испытаний и заключения по результатам аттестации объектов вычислительной техники на соответствие требованиям по защите информации) |
| ОПК-12.3.2.6 | умеет оформлять аттестат соответствия объектов вычислительной техники требованиям по защите информации |

**Раздел 5. ПРИМЕРНАЯ СТРУКТУРА И СОДЕРЖАНИЕ ОПОП**

**5.1. Рекомендуемый объем обязательной части образовательной программы.**

Объем обязательной части программы специалитета без учета объема государственной итоговой аттестации должен составлять не менее 75 процентов общего объема программы специалитета.

Рекомендуемый объем обязательной части составляет не менее 248 з.е.   
(9256 час.).

**5.2. Рекомендуемые типы практики**

Типы учебной практики:

учебно-лабораторный практикум;

ознакомительная практика;

экспериментально-исследовательская практика.

Типы производственной практики:

проектно-технологическая практика;

эксплуатационная практика;

научно-исследовательская работа;

преддипломная практика.

Преддипломная практика проводится для выполнения выпускной квалификационной работы и является обязательной.

**5.3. Примерный учебный план и примерный календарный учебный график**

Примерный учебный план и примерный календарный учебный график приведены в приложениях 3 и 4.

**5.4. Примерные программы дисциплин (модулей) и практик**

**Б.1.О.1. Дисциплина «История» («История России», «Всеобщая история»)**

Коды формируемых компетенций: ОПК-17*.*

В результате изучения дисциплины студент должен

знать:

- периодизацию, основные факты, явления и процессы всемирной и отечественной истории;

- особенности исторического пути России, ее место и роль в мировом сообществе в контексте всеобщей истории;

уметь:

- анализировать основные этапы и закономерности исторического развития России, в том числе для формирования гражданской позиции и развития патриотизма.

Примерное распределение часов: трудоемкость дисциплины 4 з.е., 144 час.

Форма контроля: экзамен.

Содержание дисциплины:

**Становление и развитие русского государства** (X – сер. XV вв.). **Основные тенденции и особенности развития Российского централизованного государства** (XV–XVII вв.). **Российская империя**: вехи истории (XVIII – конец XIX вв.). **Россия в период исторических потрясений**. СССР в период построения «социализма в отдельно взятой стране». Основные тенденции развития современной России в конце ХХ – начале XXI вв.

**Б.1.О.2. Дисциплина «Физическая культура»**

Коды формируемых компетенций: УК-7*.*

В результате изучения дисциплины студент должен

знать:

- основы теории и методики физического воспитания;

- основы организации и проведения самостоятельных занятий по физической подготовке;

уметь:

- переносить физическую нагрузку и психологическое напряжение, возникающее в связи с ней.

Примерное распределение часов: трудоемкость дисциплины 2 з.е., 72 час.

Форма контроля: 2 зачета.

Содержание дисциплины:

**Теоретические основы физической культуры.** Планирование, организация, контроль и учет физической подготовки. Средства и методы физической подготовки. Формы проведения физической подготовки. Учебные занятия, утренняя физическая зарядка, спортивно-массовая работа. Физическая тренировка в процессе учебной деятельности. Самостоятельная тренировка. **Основные разделы физической подготовки:** гимнастика и атлетическая подготовка, ускоренное передвижение и лёгкая атлетика, спортивные и подвижные игры.

**Б.1.О.3. Дисциплина «Иностранный язык»**

Коды формируемых компетенций: УК-4*.*

В результате изучения дисциплины студент должен

знать:

- основные фонетические особенности, лексический минимум, грамматический строй иностранного языка для устной и письменной коммуникации в сфере профессиональной деятельности;

уметь:

- вести диалогическую и монологическую речь в основных ситуациях профессионального общения на иностранном языке, читать и переводить   
(со словарем) тексты, извлекать и использовать в профессиональной деятельности полученную информацию.

Примерное распределение часов: трудоемкость дисциплины 11 з.е., 396 час.

Форма контроля: 3 зачета, экзамен.

Содержание дисциплины:

**Язык как средство межкультурного общения.** Фонетика. Лексика. Грамматический строй. **Диалогическая и монологическая речь в основных ситуациях. Чтение и перевод текстов. Деловая переписка.**

**Б.1.О.4. Дисциплина «Экономика»**

Коды формируемых компетенций: УК-10*.*

В результате изучения дисциплины студент должен

знать:

- основные виды доходов, финансовые инструменты, виды и источники возникновения экономических и финансовых рисков в экономике;

- место, роль и функции государства в экономике, цели, задачи и инструменты бюджетно-налоговой, денежно-кредитной политики государства и их влияние на макроэкономические параметры и поведение индивидов;

- нормативные правовые акты, регламентирующие вопросы реализации бюджетно-налоговой и денежно-кредитной политики государства;

уметь:

- анализировать информацию, необходимую для принятия обоснованных экономических решений, уметь прогнозировать их последствия и применять полученные знания в сфере личного экономического и финансового планирования;

- применять нормативные правовые акты при принятии экономических решений.

Примерное распределение часов: трудоемкость дисциплины 4 з.е., 144 час.

Форма контроля: экзамен.

Содержание дисциплины:

**Место, роль и функции государства в экономике.** Цели, задачи и инструменты бюджетно-налоговой, денежно-кредитной политики государства. Основные виды доходов. Финансовые инструменты. Виды и источники возникновения экономических и финансовых рисков в экономике. **Нормативные правовые акты, регламентирующие вопросы реализации бюджетно-налоговой и денежно-кредитной политики.** Требования антикоррупционного законодательства.

**Б.1.О.5. Дисциплина «Философия»**

Коды формируемых компетенций: УК-1*.*

В результате изучения дисциплины студент должен

знать:

- содержание и взаимосвязь основных принципов, законов, понятий   
и категорий философских наук, основные этапы развития философской мысли, основную проблематику и структуру философского знания;

- понятие мировоззрения, исторические типы мировоззрения, соотношение философии и мировоззрения, соотношение философского мировоззрения и научной картины мира.

Примерное распределение часов: трудоемкость дисциплины 5 з.е., 180 час.

Форма контроля: зачет, экзамен.

Содержание дисциплины:

**Философия как особый вид знания.** Основные разделы, направления, методы и приемы философии. Философские учения, законы, категории, понятия. Структура и методология научного познания. **Сущность, специфика, методология и методы научного исследования.** Онтология и гносеология. Принципы, законы, категории диалектики и их применение в научном познании и практике. **Философия человека и общества. Философские аспекты мировых религий.**

**Б.1.О.6. Дисциплина «Безопасность жизнедеятельности»**

Коды формируемых компетенций: УК-8*.*

В результате изучения дисциплины студент должен

знать:

- опасные и вредные факторы системы «человек – среда обитания», факторы, угрожающие жизни человека в условиях чрезвычайных ситуаций и военных конфликтов;

- основные требования по охране окружающей среды, по охране труда   
и технике безопасности в профессиональной деятельности и в повседневной жизни, основные приемы оказания первой помощи;

уметь:

- использовать средства индивидуальной защиты, оказывать первую помощь при ранениях и травмах в повседневной деятельности, в условиях чрезвычайных ситуаций и военных конфликтов.

Примерное распределение часов: трудоемкость дисциплины 3 з.е., 108 час.

Форма контроля: зачет.

Содержание дисциплины:

**Комфортные и допустимые условия жизнедеятельности.** Проблема обеспечения безопасности человека в системе «человек – среда обитания», концепция рисков, опасные и вредные факторы. Микроклимат и воздушная среда рабочей зоны. Действие вредных веществ на организм человека в конкретном производстве. Нормирование концентрации вредных веществ в воздушной среде рабочей зоны. Производственный шум. Производственное освещение. Оптимизация параметров рабочих мест. Техногенные и природные чрезвычайные ситуации (ЧС): прогнозирование параметров и оценка обстановки при ЧС; защитные мероприятия при ЧС; ликвидация последствий ЧС; защита от терроризма; действия во время военных конфликтов. Охрана окружающей среды. **Охрана труда и техника безопасности.** Электробезопасность. Защита от электромагнитных полей высокой и сверхвысокой частоты. Защита от лазерных излучений. Радиационная безопасность. Пожарная безопасность. Организация работы по охране труда, пожарной и электробезопасности: виды инструктажей и их периодичность; нормативные документы и инструкции, регламентирующие организацию деятельности по охране труда, пожарной и электробезопасности. Доврачебная помощь пострадавшему: способы и средства оказания доврачебной помощи на производстве и в быту; оказание первой помощи пострадавшим от электрического тока и при других несчастных случаях, возникающих при чрезвычайных ситуациях и военных конфликтах.

Рекомендуемый перечень лабораторных работ:

1. Измерение освещенности.

2. Измерение уровня шума

3. Оценка электробезопасности на рабочем месте.

Рекомендуемый перечень основной литературы:

1. Белов С.В. Безопасность жизнедеятельности и защита окружающей среды (техносферная безопасность). – М.: Юрайт, 2013.

2. Михайлов Л.А. Безопасность жизнедеятельности: Учебник. – СПб.: Питер, 2013. – 464 с.

3. Каракиян В.И., Никулина И.М. Безопасность жизнедеятельности. Учебник. – М.: Юрайт, 2015. – 330 с.

Перечень материально-технического обеспечения:

лаборатория по безопасности жизнедеятельности, оборудованная стендами   
и установками:

- «Звукоизоляция и звукопоглощение»;

- «Эффективность и качество освещения»;

- «Электробезопасность трехфазных сетей переменного тока»;

- «Защита от СВЧ излучения»;

- тренажер оказания первой медицинской помощи.

**Б.1.О.7. Дисциплина «Управление проектами»**

Коды формируемых компетенций: УК-1, УК-2, УК-3, УК-6*.*

В результате изучения дисциплины студент должен

знать:

- основные источники информации о проблемных ситуациях в профессиональной деятельности и подходы к критическому анализу этой информации;

- порядок принятия решений при возникновении проблемных ситуаций в профессиональной деятельности;

- основные модели жизненного цикла проекта, его этапы и фазы, их характеристики и особенности;

- содержание организации и руководства деятельностью рабочего коллектива (группы);

- социально-психологические характеристики рабочего коллектива (группы);

- основы поддержания нравственных отношений в рабочем коллективе (группе);

- методы и средства самостоятельного решения задач в сфере профессиональной деятельности;

- основы деятельностного подхода;

уметь:

- критически анализировать проблемные ситуации и вырабатывать стратегию действий в ходе решения профессиональных задач;

- разрабатывать и реализовывать этапы проекта в сфере профессиональной деятельности;

- организовывать работу коллектива (группы) для решения поставленных задач в сфере профессиональной деятельности;

Примерное распределение часов: трудоемкость дисциплины 5 з.е., 180 час.

Форма контроля: зачет, экзамен.

Содержание дисциплины:

**Основы управления.** Сущность и содержание управления. Законы, принципы и требования к управлению трудовым коллективом. Функции управления. Организация руководства трудовыми коллективами. Роль планирования в управленческой деятельности. Виды планов. Контроль выполнения планов. **Управленческое решение.** Правила формулирования проблемы. Проблемная ситуация. Источники информации о проблемных ситуациях. Подходы к критическому анализу информации. Участники процесса принятия решений. Субъекты решения. Решения, принимаемые индивидуально. Решения, принимаемые группами людей. Требования к решениям. Классификация решений. Базовые концепции процесса принятия решений. Модели процесса принятия решений. Методы принятия решений. Уровни принятия решений. Этапы принятия решений. Контроль принятых решений. **Управленческая деятельность руководителя.** Сущность и содержание управленческой деятельности руководителя. Обобщенные задачи и функции руководителя. Влияние и власть, авторитет и лидерство, стили и методы работы руководителя. Этикет взаимоотношений руководителя и подчиненного. Социально-психологические характеристики рабочего коллектива и их учет. Организационная культура. Духовная культура. Поддержание организационной культуры, нравственных отношений и этикета взаимоотношений в коллективе. Конфликт в коллективе. Основные типы, причины и последствия конфликтов. Противодействие возникновению, урегулирование и разрешение конфликтов. **Понятие и сущность управления проектами.** Сущность и классификация проектов. Отличительные характеристики и признаки проекта. Концепция и базовые понятия управления проектами: команда проекта, организационная структура. Роль менеджера проекта Управление проектом как искусство. Системный подход к управлению проектами. Основные ограничения проекта. **Стандарты и методологии управления проектами.** Основные модели жизненного цикла проекта. Процессы, фазы и этапы жизненного цикла проекта, их основные характеристики. Международные и национальные стандарты управления проектами. Методологии и процедуры управления проектами. Функциональные области управления проектами: управление содержанием и объемом работ (управление целями проекта), управление временем (сроками) проекта, управление стоимостью проекта, управление качеством проекта, управление материально-техническим обеспечением (материальными ресурсами) проекта, управление человеческими ресурсами (персоналом) проекта, управление рисками проекта, управление информацией и коммуникациями в проекте, интеграционное управление проектом. **Самообразование и саморазвитие.** Принципы деятельностного подхода к самообразованию, саморазвитию и самореализации. Способы самостоятельного получения новых знаний. Методы и средства самостоятельного решения задач.

**Б.1.О.8. Дисциплина «Математический анализ»**

Коды формируемых компетенций: ОПК-3.

В результате изучения дисциплины студент должен

знать:

- основные положения теории пределов функций, теории рядов;

- основные теоремы дифференциального и интегрального исчисления функций одного и нескольких переменных;

- основные теоремы теории функций комплексного переменного;

уметь:

- решать типовые задачи на вычисление пределов функций, дифференцирование и интегрирование, на разложение функций в ряды;

- производить исследование функций, применять приложения дифференциального и интегрального исчисления;

- применять аппарат теории функций комплексного переменного, в том числе для решения задач в действительной области.

Примерное распределение часов: трудоемкость дисциплины 15 з.е., 540 час.

Форма контроля: 3 экзамена.

Содержание дисциплины:

**Множество действительных чисел. Понятие функции.** Множества, операции над множествами. Свойства операций над множествами. Понятие отображения (функции). Классификация отображений. Эквивалентность множеств. Счетные и несчетные множества. Понятие мощности. Сравнение множеств по мощности. Числовые множества. Множество действительных чисел и его свойства. Числовые промежутки. Окрестность точки. Открытые и замкнутые множества. Ограниченные и неограниченные множества. Точные грани числовых множеств. **Теория пределов числовых последовательностей и числовых рядов.** Числовые последовательности. Предел числовой последовательности. Сходимость последовательности. Ограниченные и монотонные последовательности. Простейшие свойства пределов последовательностей. Число *e*. Числовой ряд. Сходимость и расходимость числового ряда. Необходимый признак сходимости числового ряда. Арифметические свойства сходящихся числовых рядов. Критерий Коши сходимости числового ряда. Ряды с положительными членами и основные признаки их сходимости. Знакочередующиеся ряды. Признак сходимости Лейбница. Абсолютно и условно сходящиеся ряды, их свойства. **Теория пределов функций одной действительной переменной.** Предел функции по Коши и по Гейне. Односторонние пределы функций. Основные теоремы о пределах функций. Бесконечно большие и бесконечно малые функции и их свойства. Эквивалентные функции **Непрерывность функций одной действительной переменной.** Непрерывность функции в точке и на множестве. Арифметические операции над непрерывными функциями. Непрерывность сложной и обратной функций. Непрерывность элементарных функций. Замечательные пределы. Свойства функций, непрерывных на отрезке. Точки разрыва и их классификация. **Дифференциальное исчисление функций одной действительной переменной.** Производная функции. Геометрическое и механическое истолкование производной. Дифференцируемость функции, необходимые и достаточные условия дифференцируемости. Связь с непрерывностью. Понятие дифференциала функции. Простейшие свойства производных и дифференциалов. Таблица производных и дифференциалов основных элементарных функций и дифференциал суммы, произведения и частного. Производная и дифференциал сложной функции и обратной функции. Производные и дифференциалы высших порядков. Механическое истолкование второй производной. Формула Лейбница для *n*-ой производной от произведения двух функций. Дифференциалы высших порядков сложной функции. Дифференцирование функций, заданных параметрически. Простейшие формулы приближенного вычисления производных функции. Оценки погрешности. **Приложения дифференциального исчисления функций одной действительной переменной.** Теоремы Ферма, Ролля, Лагранжа, Коши. Формула Тейлора. Признаки постоянства, возрастания и убывания функции на промежутке. Экстремумы функций. Нахождение наименьшего и наибольшего значений функции на замкнутом промежутке. Правило Лопиталя-Бернулли раскрытия неопределенностей. Касательная и нормаль к плоской кривой. Исследование функций с помощью дифференциального исчисления. **Функции многих действительных переменных. Теория пределов, непрерывность.** Действительное *n*-мерное арифметическое пространство. Понятие расстояния в действительном *n-*мерном арифметическом пространстве. Предельные, внутренние и граничные точки. Открытые и замкнутые множества. Понятие функции многих переменных. Предел и непрерывность. **Дифференцируемость функции многих действительных переменных.** Частные производные функций многих переменных. Частные производные высших порядков. Дифференцируемые функции. Признак дифференцируемости. Касательная плоскость и нормаль к поверхности. Геометрический смысл дифференциала. Дифференцируемость сложной функции. Дифференциалы высших порядков. Производная по направлению. Понятие и свойства градиента функции. Формула Тейлора для функций многих переменных. Понятие об экстремумах функций многих переменных. **Интегральное исчисление. Неопределенный интеграл.** Первообразная функция. Неопределенный интеграл и его основные свойства. Таблица неопределенных интегралов от основных элементарных функций. Основные методы интегрирования. **Определенный интеграл.** Задача вычисления площади криволинейной трапеции и другие задачи, приводящие к понятию определенного интеграла. Формула Ньютона-Лейбница. Интеграл Римана (определенный интеграл). Простейшие свойства определенного интеграла. Существование первообразной непрерывной функции. Замена переменной. Геометрические приложения. Интегральные суммы. Основные приемы приближенного интегрирования. Обобщенная первообразная. Интегралы от разрывных функций. Несобственные интегралы. Абсолютная сходимость. Признаки сходимости. **Кратные интегралы.** Простейшие сведения об интегралах, зависящих от параметра и их свойствах. Эйлеровы интегралы. Двойной интеграл и его основные свойства. Сведение двойного интеграла к повторному интегралу. Теорема о среднем значении. Замена переменных, переход в двойном интеграле к полярным координатам. Тройной интеграл и его свойства. Сведение тройного интеграла к повторному интегралу. Замена переменных, переход в тройном интеграле к цилиндрическим и сферическим координатам. Понятие о многократных интегралах. **Криволинейные и поверхностные интегралы.** Криволинейные интегралы I и II рода. Вычисление и простейшие свойства криволинейных интегралов. Понятие о поверхностных интегралах. Элементы теории поля. **Основные понятия теории функций комплексной переменной.** Комплексные числа и функции комплексной переменной. Предел и непрерывность. Числовые ряды с комплексными членами. **Дифференцирование и интегрирование функций комплексной переменной.** Производная. Условия Коши-Римана (Даламбера-Эйлера) дифференцируемости функций комплексной переменной. Гармонические функции и их связь с аналитическими функциями. Геометрический смысл аргумента и модуля производной. Интегралы от комплекснозначных функций действительной и комплексной переменной. Простейшие свойства. Теорема Коши. Интегральная формула Коши. **Дифференциальные уравнения. Дифференциальные уравнения первого порядка.** Основные определения. Частное и общее решение. Интегральные кривые. Геометрический смысл дифференциального уравнения первого порядка. Методы решения простейших дифференциальных уравнений первого порядка. **Линейные дифференциальные уравнения *n*-го порядка.** Линейное однородное уравнение. Фундаментальная система решений. Определитель Вронского. Неоднородное линейное уравнение, вид общего решения. Метод вариации произвольных постоянных. Линейное уравнение с постоянными коэффициентами. Характеристическое уравнение. Общее решение. **Элементы операционного исчисления.** Интеграл Лапласа. Нахождение оригиналов и изображений. Простейшие свойства преобразования Лапласа. Приложения преобразования Лапласа к решению дифференциальных и интегральных уравнений (операторный метод). **Элементы теории функциональных рядов. Функциональные последовательности и ряды в действительной области.** Основные понятия теории функциональных рядов. Равномерная сходимость функционального ряда. Непрерывность, дифференцируемость и интегрируемость суммы функционального ряда. Степенные ряды. Теоремы Абеля. Радиус сходимости. Непрерывность, дифференцируемость и интегрируемость суммы степенного ряда. Ряд Тейлора. Разложение в ряд Маклорена основных элементарных функций. Применение степенных рядов к решению дифференциальных уравнений. **Функциональные ряды в комплексной области.** Степенные ряды с комплексными членами. Ряд Тейлора. Показательная и логарифмическая функции. Тригонометрические функции. Ряд Лорана. Изолированные особые точки. Разложение функции в ряд Лорана **Теория вычетов.** Вычет относительно полюса. Теорема Коши о вычетах. Вычисление интегралов с помощью вычетов. **Ряды Фурье. Преобразование и интеграл Фурье.** Основные задачи гармонического анализа. Ортогональные системы функций. Тригонометрическая система функций. Ряд Фурье. Признаки сходимости рядов Фурье. Неравенство Бесселя и равенство Парсеваля. Метод Фурье решения дифференциальных уравнений в частных производных. Преобразование и интеграл Фурье. Спектральная функция.

Рекомендуемый перечень основной литературы:

1. Бугров Я.С., Никольский С.М. Высшая математика в 3-х томах. – М.: «Юрайт», 2015.

2. Демидович Б.П. Задачи и упражнения по математическому анализу для ВТУЗов. – М.: «АСТ», 2010.

**Б.1.О.9. Дисциплина «Теория вероятностей и математическая статистика»**

Коды формируемых компетенций: ОПК-3.

В результате изучения дисциплины студент должен

знать:

- основные понятия и методы теории вероятностей;

- основные функциональные и числовые характеристики распределений случайных величин и случайных векторов;

- различные формы предельных теорем и методы их доказательства;

- основные понятия и методы математической статистики;

- основные характеристики и методы построения статистических оценок параметров, доверительных интервалов и статистических критериев;

уметь:

- применять стандартные методы и модели к решению теоретико-вероятностных задач в профессиональной области, в том числе применять при решении прикладных задач аппарат вероятностных распределений случайных величин;

- строить статистические модели экспериментов при решении прикладных задач, оценивать параметры статистических моделей, описывать и вычислять характеристики критериев проверки статистических гипотез.

Примерное распределение часов: трудоемкость дисциплины 6 з.е., 216 час.

Форма контроля: зачет, экзамен.

Содержание дисциплины:

**Дискретные пространства элементарных событий.** Простейшие комбинаторные задачи. Понятия события, элементарного события, суммы, произведения и разности событий. Пространство элементарных событий. Достоверное событие. Невозможное событие. Несовместные события. Вероятности элементарных событий. Дискретное пространство элементарных событий. Классическая вероятность. Описание комбинаторных задач на языке пространств элементарных событий. Вероятность дополнительного события. Вероятность объединения событий. **Комбинаторные задачи теории вероятностей.** Размещения, сочетания, перестановки для выборок с возвращением и без возвращения. Схема испытаний Бернулли. Понятие дискретной случайной величины. Понятия и свойства распределения вероятностей, функции распределения вероятностей. Полиномиальная схема испытаний. **Произвольное вероятностное пространство.** Особенности построения вероятностные пространств с несчётным числом событий. Произвольное вероятностное пространство: σ-алгебра событий и σ-аддитивная вероятностная функция на ней. Свойства вероятности. Аксиоматика Колмогорова теории вероятностей. **Условная вероятность. Независимость событий.** Условная вероятность. Независимость двух событий, попарная независимость и независимость в совокупности. Априорные и апостериорные вероятности гипотез (событий). Формула полной вероятности. Формулы Байеса. **Случайные величины и их распределения.** Типы случайных величин. Функция распределения случайной величины и её свойства. Математическое ожидание и дисперсия случайной величины. Независимые случайные величины. Совместное распределение вероятностей независимых случайных величин. Основные дискретные распределения: биномиальное, геометрическое, пуассоновское, гипергеометрическое. Математические ожидания и дисперсии этих распределений. Производящая функция дискретного распределения с целочисленной областью определения. Распределение суммы независимых целочисленных случайных величин. Непрерывные случайные величины. Понятие измеримой функции и необходимость его введения. Основные абсолютно-непрерывные распределения: нормальное, экспоненциальное, равномерное на отрезке, распределение Коши. Математические ожидания и дисперсии этих распределений. Характеристическая функция непрерывной случайной величины. Совместная функция и плотность распределения вероятностей компонентов случайного вектора. Плотность распределения случайного вектора с независимыми компонентами. Характеристическая функция суммы независимых абсолютно-непрерывных случайных величин. **Числовые характеристики случайных величин.** Начальные и центральные моменты случайных величин. Неравенство Чебышёва. Смешанные начальные и центральные моменты случайных величин. Корреляция, ковариация, коэффициент корреляции, их свойства. Вектор средних значений и ковариационная матрица случайного вектора. Многомерное нормальное распределение. **Операции над случайными величинами.** Распределение функции от случайных величин. Распределение суммы (разности) и произведения (частного) случайных величин. Формула свёртки. Распределение наибольшей (наименьшей) компоненты случайного вектора. Распределение полярных координат точки на плоскости со случайными независимыми декартовыми координатами, распределёнными по нормальному закону. **Предельные теоремы.** Виды сходимости случайных величин и соотношения между ними. Закон больших чисел. Теоремы Маркова, Чебышёва, Хинчина. Закон больших чисел для схемы испытаний Бернулли. Центральная предельная теорема. Центральная предельная теорема для независимых одинаково распределённых случайных величин. Теорема Ляпунова. **Случайные процессы.** Понятие случайного процесса. Классификация случайных процессов. Функции и плотности распределений случайных процессов. Числовые характеристики случайных процессов. Стационарные процессы. Корреляционная функция и её свойства. Энергетический спектр (спектральная плотность мощности) случайного процесса. Теорема Винера-Хинчина. Дискретные цепи Маркова. Начальное распределение, матрица переходных вероятностей и её свойства. Уравнение Колмогорова-Чепмена. Корреляционная функция дискретной цепи Маркова. Точечные случайные процессы. Процессы с независимыми приращениями. Пуассоновский случайный процесс. Распределение числа случайных событий за заданное время. Распределение времени между последовательными событиями пуассоновского потока. Гауссовские случайные процессы. Винеровский случайный процесс. Определение марковского случайного процесса с непрерывным временем. **Математическая статистика. Точечные и интервальные оценки параметров распределений.** Статистическая ситуация. Основные задачи математической статистики. Генеральная совокупность, выборка, случайная выборка, вариационный ряд, статистический ряд, статистика. Распределение крайних членов вариационного ряда. Порядковые статистики, выборочное среднее, выборочная дисперсия, эмпирическая функция распределения, гистограмма. Точечные оценки неизвестных параметров распределений. Несмещённые и состоятельные оценки. Несмещённость выборочного среднего, смещённость выборочной дисперсии. Исправленная выборочная дисперсия. Неравенство Рао-Крамера. Эффективные и асимптотически эффективные оценки. Граница Рао-Крамера для выборочного среднего нормальной генеральной совокупности. Эмпирические моменты. Метод моментов для получения оценок, свойства полученных оценок. Функция правдоподобия. Метод максимального правдоподобия для получения оценок, свойства полученных оценок. Интервальное оценивание неизвестных параметров. Доверительные интервалы и доверительные вероятности. **Основы теории принятия решений.** Постановка задачи принятия решений: пространство действий, пространство решений, функция потерь, априорная информация. Критерии оптимальности. Минимаксный критерий. Критерий минимума среднего (байесовского) риска. Задача проверки простой гипотезы против простой альтернативы как задача принятия решений. Ошибки первого и второго рода. Лемма Неймана-Пирсона. Оценка неизвестного параметра при квадратичной функции потерь. Апостериорное среднее. Оценка математического ожидания генеральной совокупности с нормальным распределением. Оценка неизвестного параметра при модульной функции потерь. Оценка математического ожидания генеральной совокупности с нормальным распределением. Медиана распределения. Оценка неизвестного параметра при простой функции потерь. Оценка максимального правдоподобия. Оценка математического ожидания генеральной совокупности с нормальным распределением. **Оценка параметров линейной регрессии.** Условное нормальное распределение. Понятие регрессии. Линейная регрессия. Оценка параметров линейной регрессии при нормальном распределении генеральной совокупности методом максимального правдоподобия. Метод наименьших квадратов. Оценка параметров линейной регрессии методом наименьших квадратов. Несмещённость оценок. Матрица дисперсий ошибок. Матрица Фишера. Интервальная оценка параметров линейной регрессии. Адекватность модели. Понятие о критериях согласия. Критерий χ-квадрат.

Рекомендуемый перечень основной литературы:

1. Гнеденко Б.В. Курс теории вероятностей. – М., Либроком, 2011.

2. Ивченко Г.И., Медведев Ю.И. Введение в математическую статистику. – М., ЛКИ, 2010.

3. Хуснутдинов Р. Теория вероятностей и математическая статистика. Сборник задач. Учебное пособие. – М.: Лань, 2014.

**Б.1.О.10. Дисциплина «Алгебра и геометрия»**

Коды формируемых компетенций: ОПК-3.

В результате изучения дисциплины студент должен

знать:

- основные положения теории матриц, методы решения систем линейных уравнений;

- основные понятия аналитической геометрии;

- основные алгебраические структуры и методы работы с ними;

- основные понятия векторной алгебры, в том числе линейные векторные и евклидовые пространства и их линейные преобразования;

уметь:

- пользоваться методами описания объектов средствами аналитической геометрии;

- использовать основные методы линейной и общей алгебры для решения типовых задач дискретной математики.

Примерное распределение часов: трудоемкость дисциплины 5 з.е., 180 час.

Формы контроля: зачет, экзамен.

Содержание дисциплины:

**Матрицы и определители над полем вещественных чисел.** Виды матриц, линейные операции и их свойства. Умножение матриц и его свойства. Операции с матрицами. Определитель матрицы, определение и свойства. Вычисление определителей. Подматрицы, миноры, алгебраические дополнения. Обратная матрица, критерий обратимости. Методы нахождения обратных матриц. Элементарные преобразования, эквивалентность матриц. Приведение матриц к стандартным формам. **Арифметические пространства и системы линейных уравнений.** Линейная зависимость векторов, свойства, теорема о ранге. Подпространства арифметических пространств. Свойства линейно независимых систем. Методы решения систем линейных уравнений, критерии совместности и определенности, общее решение системы однородных линейных уравнений, фундаментальная система решений. **Аналитическая геометрия на плоскости и в пространстве.** Векторная алгебра. Свойства операций над векторами. Системы координат, уравнения линии и поверхности. Прямая на плоскости, прямая и плоскость в пространстве. Свойства прямых и плоскостей. Линии второго порядка на плоскости. Уравнения эллипса, гиперболы и параболы, их свойства. Поверхности второго порядка в пространстве. **Группы, кольца и поля.** Основные определения и свойства. Числовые кольца и поля. Отношение делимости целых чисел. Деление с остатком. Наибольший общий делитель и наименьшее общее кратное целых чисел. Алгоритм Евклида. Простые числа. Основная теорема арифметики. Каноническое разложение числа. **Поле комплексных чисел.** Возведение в степень и извлечение корня из комплексного числа. **Кольца вычетов.** Сравнение целых чисел по модулю. Свойства отношения сравнимости. Построение кольца классов вычетов по заданному модулю. Описание обратимых элементов и делителей нуля в этом кольце. Функция Эйлера и ее свойства. Решение сравнений. Китайская теорема об остатках. Решение сравнений и систем сравнений. **Кольцо многочленов над полем.** Операции с многочленами. Кольцо многочленов над кольцом с единицей. Делимость многочленов. Деление многочленов с остатками. Теорема Безу. Наибольший общий делитель и наименьшее общее кратное многочленов над полем. Алгоритм Евклида нахождения наибольшего общего делителя двух многочленов. Неприводимые многочлены над полем. Каноническое разложение многочлена. Отношение сравнимости многочленов и его свойства. Кольцо классов вычетов. Построение полей заданного порядка. **Линейные векторные пространства.** Определение линейного пространства. Линейная зависимость векторов линейного пространства и ее свойства. Базисы линейных пространств. Координаты векторов в базисе. Матрица перехода. Формулы преобразования координат. Подпространства линейных пространств. Евклидовы пространства. Длины векторов и расстояния между векторами. Ортогонализация Грама-Шмидта. Подпространства евклидовых пространств. Нахождение ортогональной проекции и ортогональной составляющей вектора относительно заданного подпространства. **Линейные преобразования векторных пространств.** Определение и свойства линейного преобразования. Матрица линейного преобразования в базисе пространства. Подобие матриц. Общие свойства линейных преобразований. Характеристический многочлен линейного преобразования. Собственные векторы и собственные значения. Критерий подобия матрицы диагональной. Ядро и образ линейного преобразования. Инвариантные подпространства. Распавшиеся и полураспавшиеся матрицы. Разложение пространства в прямую сумму инвариантных подпространств. **Линейные преобразования евклидовых пространств.** Сопряженное преобразование, его матрица, нормальные преобразования. Матрица сопряженного преобразования. Самосопряженные преобразования, их свойства. Приведение к главным осям. Ортогональные преобразования и их свойства. Приведение матрицы ортогонального преобразования к блочно-диагональному виду. **Квадратичные формы.** Общие свойства квадратичных форм. Метод Лагранжа приведения квадратичной формы к каноническому виду. Действительные квадратичные формы. Критерий Сильвестра.

Рекомендуемый перечень основной литературы:

1. Ильин В.А., Позняк Э.Г. Аналитическая геометрия. – М.: ФИЗМАТЛИТ, 2012.

2. Беклемишева Л.А., Беклемишев Д.В., Петрович А.Ю., Чубаров И.А. Сборник задач по аналитической геометрии и линейной алгебре. – М.: Лань, 2016.

3. Кострикин А.И. Введение в алгебру в 3 частях. Часть 1. Основы алгебры. – М.: МЦНМО, 2012.

**Б.1.О.11. Дисциплина «Дискретная математика»**

Коды формируемых компетенций: ОПК-3.

В результате изучения дисциплины студент должен

знать:

- основные положения и методы комбинаторики, теории графов и элементы теории булевых функции;

- элементы теории кодов и теории автоматов;

уметь:

- пользоваться методами дискретной математики для решения задач профессиональной деятельности.

Примерное распределение часов: трудоемкость дисциплины 4 з.е., 144 час.

Форма контроля: экзамен.

Содержание дисциплины:

**Основы комбинаторики.** Принципы комбинаторики: принцип сложения и принцип умножения. Основные комбинаторные объекты: размещения, сочетания, перестановки, размещения с повторениями, сочетания с повторениями и их число. Биномиальные коэффициенты и их свойства. Основные комбинаторные тождества. Подсчет числа отношений эквивалентности, в том числе заданного ранга. Метод включений и исключений. Метод рекуррентных соотношений. **Элементы теории графов.** Основные понятия теории графов. Способы задания графов. Числовые характеристики графов. Пути и циклы в графах. Матрица смежности графа. Компоненты связности. Изоморфизм графов. Эйлеровы графы. Гамильтоновы графы. Деревья и их свойства. Остовные деревья и остовы несвязных графов. Прикладные задачи и алгоритмы анализа графов. **Булевы функции.** Совершенные дизъюнктивные и конъюнктивные нормальные формы. Представление функции полиномом Жегалкина и способы его нахождения. Классы Поста. Замкнутость и полнота системы булевых функций, критерий полноты. Базисы булевых функций, число функций в базисе. Шефферовы функции, их число. **Конечные автоматы.** Автоматы и автоматные отображения. Подавтоматы. Способы задания автоматов и операции с ними. Основные примеры автоматов. Граф автомата и его подавтомата. Построение схем из функциональных элементов. Изоморфизм автоматов. Эквивалентность состояний конечного автомата. Эквивалентные автоматы. Минимальный автомат и способ построения минимального автомата, эквивалентного данному. **Основы теории кодирования.** Основные понятия теории кодирования. Блоковые коды. Основные оценки параметров блоковых кодов. Линейные коды. Способы задания линейных кодов, нахождение параметров. Двойственные коды. Тождество Мак-Вильямс. Циклические коды.

Рекомендуемый перечень основной литературы:

1. Асанов М.О., Баранский В.А., Расин В.В. Дискретная математика: графы, матроиды, алгоритмы. – СПб.: Лань, 2010.

2. Гаврилов Г.П. Сапоженко А.А. Задачи и упражнения по курсу дискретной математики. – М.: Физматлит, 2005.

3. Галкина В.А. Дискретная математика: комбинаторные методы оптимизации. – М.: Гелиос АРВ, 2003.

5. Яблонский С.В. Введение в дискретную математику: учебное пособие для вузов. – М.: Высшая школа, 2006.

6. Белоусов А.И., Ткачев С.Б. Дискретная математика. – М.: изд. МГТУ им. Н.Э. Баумана, 2015.

**Б.1.О.12. Дисциплина «Физика»**

Коды формируемых компетенций: ОПК-4.

В результате изучения дисциплины студент должен

знать:

- основные законы механики;

- основные законы термодинамики и молекулярной физики;

- основные законы электричества и магнетизма;

- основы теории колебаний и волн, волновой оптики;

- основы квантовой оптики, квантовой механики;

уметь:

- использовать математические модели физических явлений и процессов;

- решать типовые прикладные физические задачи;

- проводить физический эксперимент, обрабатывать его результаты и делать выводы о проделанной исследовательской работе.

Примерное распределение часов: трудоемкость дисциплины 18 з.е., 648 час.

Форма контроля: 3 экзамена.

Содержание дисциплины:

**Механика материальной точки.** Кинематика материальной точки и абсолютно твердого тела: вычисление пройденного пути; ускорение; компоненты ускорения по декартовым координатным осям; тангенциальное, нормальное и полное ускорения (для плоского движения материальной точки); кинематика вращательного движения абсолютно твердого тела; угловая скорость и угловое ускорение; связь между угловыми и линейными скоростями и ускорениями; кинематика плоского движения абсолютно твердого тела; мгновенная ось вращения. Динамика материальной точки: инерциальная система отсчета; законы Ньютона; границы применимости классической механики; основная задача механики; задача Коши; преобразования Галилея; принцип относительности Галилея. Законы сохранения: сохраняющиеся величины; аддитивные интегралы движения; связь законов сохранения со свойствами пространства и времени; работа и мощность; работа центральных сил и сил однородного силового поля; потенциальная энергия частицы во внешнем (центральном и однородном) поле сил; связь между потенциальной энергией и силой; градиент; свойства градиента; кинетическая энергия материальной точки и системы материальных точек; связь кинетической энергии материальной точки с работой всех сил, действующих на материальную точку; закон сохранения полной механической энергии для частицы, движущейся в консервативном поле сил; импульс материальной точки и системы материальных точек; закон сохранения импульса системы взаимодействующих материальных точек; центр масс; движение центра масс системы материальных точек; система центра масс; момент импульса материальной точки (системы материальных точек) относительно точки и относительно оси; момент силы относительно точки и относительно оси; закон сохранения момента импульса системы взаимодействующих материальных точек. Неинерциальные системы отсчета: неинерциальные системы отсчета; силы инерции; законы сохранения в неинерциальных системах отсчета. **Механика твердого тела.** Механика твердого тела: законы динамики твердого тела; момент импульса твердого тела, вращающегося вокруг неподвижной оси; момент инерции; теорема Гюйгенса-Штейнера; вычисление моментов инерции; кинетическая энергия тела, вращающегося вокруг неподвижной оси; работа, совершаемая внешними силами при вращении твердого тела относительно неподвижной оси; кинетическая энергия тела при плоском движении; гироскоп; прецессия гороскопа. Механические колебания: гармонические колебания; энергия гармонического колебания; собственные механические колебания; затухающие колебания; логарифмический декремент затухания; добротность колебательной системы. Элементы специальной теории относительности: принцип относительности Эйнштейна; принцип постоянства скорости света; преобразования Лоренца и следствия из них; интервал; его инвариантность относительно преобразований Лоренца; мировая точка; мировая линия; релятивистское преобразование скоростей; релятивистское выражение для импульса; релятивистское выражение для энергии; релятивистское преобразование энергии-импульса. **Статистическая термодинамика.** Молекулярная физика и термодинамика: термодинамический и статистический методы исследования системы многих тел; уравнение состояния идеального газа; состояние термодинамической системы; процесс; основные законы (начала) термодинамики; первое начало термодинамики; внутренняя энергия идеального газа; работа, совершаемая идеальным газом; частные случаи (изобарический, изохорический, изотермический процессы); теплоемкость идеального газа при постоянном объеме и при постоянном давлении; соотношение Майера; адиабатический процесс; уравнение адиабаты идеального газа; работа, совершаемая идеальным газом при адиабатическом процессе; политропический процесс; уравнение политропы идеального газа; показатель политропы; теплоемкость идеального газа при политропическом процессе; работа, совершаемая идеальным газом при политропическом процессе; энтропия идеального газа; второе начало термодинамики; КПД циклов; цикл Карно; уравнение Ван-дер-Ваальса; внутренняя энергия Ван-дер-Ваальсовского газа; изотермы Ван-дер-Ваальса; реальные изотермы. Статистическая физика: различные формы записи уравнения состояния идеального газа; средняя энергия молекул; степени свободы; закон равнораспределения; число ударов молекул газа о стенку сосуда; давление газа на стенку сосуда; статистическое толкование термодинамических параметров - температуры и давления; элементарные сведения из теории вероятностей; распределение максвелла; наиболее вероятная скорость молекул газа; средняя скорость молекул газа; средняя квадратичная скорость молекул газа; барометрическая формула; распределение Больцмана; распределение Максвелла-Больцмана; статистическое толкование энтропии; микросостояние; макросостояние; статистический вес; связь энтропии системы со статистическим весом состояния системы. **Электричество.** Электрическое поле в вакууме: электрический заряд; закон сохранения электрического заряда; закон Кулона; электрическое поле; вектор напряженности электрического поля; принцип суперпозиции электрических полей; основная задача электростатики; работа сил электростатического поля; потенциал; связь между потенциалом и вектором напряженности электрического поля; энергия взаимодействия системы зарядов; поле системы зарядов на больших расстояниях; дипольный электрический момент системы зарядов; электрический диполь; электрический момент диполя; поле диполя; электрический диполь во внешнем электрическом поле; теорема Гаусса для электростатического поля; теорема о циркуляции вектора напряженности электростатического поля; применение теоремы Гаусса при решении основной задачи электростатики. Электрическое поле в диэлектриках: поляризация диэлектриков; электрическое поле в диэлектриках; объемные и поверхностные связанные заряды; вектор поляризованности диэлектрика и его свойства; вектор электрического смещения; диэлектрическая проницаемость среды; теорема Гаусса для поля вектора; условия на границе двух диэлектриков; примеры на вычисление полей в диэлектриках. Проводники в электрическом поле: электростатика проводников; условие равновесия зарядов на проводнике; проводник во внешнем электрическом поле; электроемкость уединенного проводника; конденсаторы; емкость конденсатора; соединения конденсаторов; расчет емкости конденсаторов различных конфигураций. Энергия электрического поля: Энергия электрического поля; плотность энергии электрического поля. Постоянный электрический ток: электрический ток; уравнение непрерывности; электродвижущая сила; электрическое поле проводника с током; закон ома для однородного и неоднородного участка цепи; разветвленные цепи постоянного тока; правила Кирхгофа; переходные процессы в цепи с конденсатором; работа и мощность тока; закон Джоуля-Ленца. **Магнетизм.** Магнитное поле в вакууме: магнитное поле; вектор магнитной индукции; закон Био-Савара-Лапласа; принцип суперпозиции магнитных полей; силовые линии магнитного поля; основная задача магнитостатики; магнитное поле движущегося заряда; сила Лоренца; движение заряженных частиц в магнитном поле; сила ампера; сила взаимодействия параллельных токов; поток и циркуляция вектора магнитной индукции; контур с током в магнитном поле; дипольный магнитный момент контура с током; магнитное поле контура с током; работа, совершаемая при перемещении тока в магнитном поле; элементы векторного анализа; дивергенция и ротор магнитного поля; теорема Стокса; теорема о циркуляции вектора магнитной индукции. Магнитное поле в веществе: намагничение магнетика; вектор намагниченности; циркуляция и ротор вектора намагниченности; вектор напряженности магнитного поля; магнитная восприимчивость; магнитная проницаемость вещества; теорема о циркуляции вектора напряженности магнитного поля; условия на границе двух магнетиков; виды магнетиков; диамагнетики, парамагнетики и ферромагнетики. Электромагнитная индукция: явление электромагнитной индукции; закон электромагнитной индукции Фарадея; правило Ленца; электродвижущая сила индукции; токи Фуко; скин-эффект; явление самоиндукции; индуктивность; взаимная индукция; ток при замыкании и размыкании цепи с индуктивностью; энергия магнитного поля. Уравнения Максвелла: вихревое электрическое поле; ток смещения; уравнения Максвелла. Электрические колебания. Переменный ток: квазистационарные токи; свободные гармонические колебания в колебательном контуре без активного сопротивления; свободные затухающие колебания в контуре; вынужденные колебания в контуре; резонанс; переменный электрический ток; импеданс; реактивные сопротивления; действующие значения тока и напряжения. **Волны.** Упругие волны: распространение волн в упругой среде; волновое уравнение; уравнение волны; энергия упругой волны; вектор Умова. Электромагнитные волны: волновое уравнение электромагнитного поля; плоская электромагнитная волна; энергия и импульс электромагнитного поля; вектор Пойнтинга; излучение диполя; эффект Доплера для электромагнитных волн. Фотометрия: световой поток; фотометрические величины и единицы. **Оптика.** Интерференция света: интерференция световых волн; когерентность; способы наблюдения интерференции света; многолучевая интерференция. Дифракция света: дифракция света; принцип Гюйгенса-Френеля; зоны Френеля; дифракция Френеля от простейших преград; волновой параметр; дифракция Фраунгофера на щели; дифракционная решетка; угловая дисперсия и разрешающая сила спектрального прибора; критерий Рэлея; дифракция рентгеновских лучей. Поляризация света: естественный и поляризованный свет; поляризация света при отражении и преломлении; закон Брюстера; формулы Френеля; поляризация при двойном лучепреломлении; интерференция поляризованных волн; прохождение плоскополяризованного света через кристаллическую пластинку; кристаллическая пластинка между двумя поляризаторами; искусственное двойное лучепреломление; вращение плоскости поляризации. Дисперсия света: дисперсия света; групповая скорость; элементарная теория дисперсии; поглощение света; закон Бугера; рассеяние света. **Квантовая оптика.** Тепловое излучение: тепловое излучение; закон Кирхгофа; формула Рэлея-Джинса; формула Планка; закон Стефана-Больцмана; закон смещения Вина. Фотоны: Тормозное рентгеновское излучение; внешний фотоэффект; фотоны; эффект Комптона. **Квантовая механика.** Боровская теория атома: закономерности в атомных спектрах; обобщенная формула Бальмера; опыты по рассеянию α- частиц; ядерная модель атома Резерфорда; атом Резерфорда-Бора; постулаты Бора; элементарная теория водородного атома; условие квантования Бора Зоммерфельда; опыт Франка и Герца. Элементы квантовой механики: гипотеза де Бройля; волновые свойства вещества; дифракция электронов; принцип неопределенностей; состояние частицы в квантовой теории; принцип суперпозиции состояний; основные постулаты квантовой механики; смысл и свойства ψ-функции; плотность вероятности; нормировка; уравнение Шредингера; операторы в квантовой механике; принцип соответствия; коммутационные соотношения операторов; принцип неопределенностей и коммутационные соотношения операторов; скобки Пуассона; квантование энергии; задача на определение собственных функций и собственных значений энергии частицы в бесконечно высокой одномерной потенциальной яме; квантование момента импульса; задача на определение собственных функций и собственных значений энергии плоского ротатора; частица в центрально-симметричном поле; квантование момента импульса; задача на определение собственных функций и собственных значений операторов момента импульса и проекции момента импульса; азимутальное и магнитное квантовые числа; правило сложения моментов; прохождение частиц через потенциальный барьер; туннельный эффект; оператор плотности потока в квантовой механике; коэффициенты прохождения и отражения. Физика атомов. Периодическая система элементов Менделеева: квантование момента импульса; атом водорода; мультиплетность спектров и спин электрона; спин-орбитальное взаимодействие; результирующий механический момент многоэлектронного атома; магнитный момент атома; принцип Паули; распределение электронов по энергетическим уровням атома. Атом в магнитном поле: атом в магнитном поле; опыт Штерна-Герлаха. простой эффект Зеемана; сложный эффект Зеемана; эффект Пашена-Бака.

Рекомендуемый перечень лабораторных работ:

1. Изучение динамики поступательного движения твердых тел с помощью машины Атвуда.

2. Определение ускорения свободного падения тел с помощью оборотного маятника.

3. Изучение динамики плоского движения твердых тел с помощью маятника Максвелла.

4. Экспериментальное подтверждение закона Дюлонга и Пти.

5. Исследование собственных колебаний в простом колебательном контуре.

6. Определение диэлектрической проницаемости твердых тел.

7. Изучение переходных процессов в цепи электрического тока.

8. Изучение вихревого электрического поля.

9. Изучение интерференции с помощью бипризмы Френеля.

10. Методы получения и исследования дифракционной картины.

11. Изучение прозрачной дифракционной решетки с помощью гониометра.

12. Экспериментальное подтверждение закона Стефана-Больцмана.

13. Изучение внешнего фотоэффекта.

14. Изучение дифракции электронов.

Рекомендуемый перечень основной литературы:

1. Савельев И.В. Курс общей физики. В 5 тт. Т.1. Механика. – СПб.: Лань, 2011. – 448 с.

2. Савельев И.В. Курс общей физики. В 5 тт. Т.2. Электричество и магнетизм. – СПб.: Лань, 2011. – 348 с.

3. Савельев И.В. Курс общей физики. В 5 тт. Т.3. Молекулярная физика и термодинамика. – СПб.: Лань, 2011. – 224 с.

4. Савельев И.В. Курс общей физики. В 5 тт. Т.4. Волны. Оптика. – СПб.: Лань, 2011. – 256 с.

5. Савельев И.В. Курс общей физики. В 5 тт. Т.5. Квантовая оптика. Атомная физика. Физика твердого тела. Физика атомного ядра и элементарных частиц. – СПб.: Лань, 2011. – 384 с.

6. Савельев И.В. Сборник вопросов и задач по общей физике. – СПб.: Лань, 2013. – 288 с.

7. Иродов И.Е. Задачи по общей физике. – М.: ЛБЗ, 2010.

Перечень материально-технического обеспечения:

лаборатория физики, оснащенная учебно-лабораторными стендами по механике, электричеству и магнетизму, электродинамике, оптике.

**Б.1.О.13. Дисциплина «Электроника и схемотехника»**

Коды формируемых компетенций: ОПК-4.

В результате изучения дисциплины студент должен

знать:

- принципы действия и характеристики электронных компонентов телекоммуникационных систем;

- типовые схемотехнические решения основных узлов и блоков электронной аппаратуры;

- методы анализа электронных схем;

- основные правила выполнения и оформления электрических схем;

уметь:

- анализировать элементную базу электронной аппаратуры;

- работать с программными средствами схемотехнического моделирования и использовать измерительную технику при экспериментальном исследовании электронной аппаратуры.

Примерное распределение часов: трудоемкость дисциплины 8 з.е., 288 час.

Форма контроля: зачет, экзамен.

Содержание дисциплины:

**Элементная база полупроводниковой электроники.** Полупроводники: основные параметры полупроводников; электронно-дырочный переход; прямое смещение *p*-*n* перехода; обратное смещение *p*-*n* перехода; вольтамперная характеристика p-n перехода; емкости *p*-*n* перехода. Полупроводниковые диоды: основные типы полупроводниковых диодов; характеристики, области применения. Принцип работы биполярного транзистора: вольтамперные характеристики биполярного транзистора; эквивалентные схемы биполярного транзистора. Основные параметры биполярных транзисторов: дифференциальные параметры транзистора; зависимость от режима по постоянному току; зависимость от частоты. Принцип работы полевых транзисторов: полевой транзистор с управляющим *p*-*n* переходом; полевой транзистор МОП- или МДП-типа; принцип действия МОП-транзистора. Разновидности полевых транзисторов. Основные параметры полевых транзисторов. Интегральные схемы (ИС): основные виды ИС; технология изготовления полупроводниковых ИС; технология изготовления пленочных ИС; примеры ИС (полупроводниковая ИС, гибридная ИС). **Электронные усилители и преобразователи сигналов.** Основные параметры и характеристики усилителей. Графический анализ усилительного каскада. Классы усиления усилителей (А, В, АВ, С, D). Обратная связь в усилителях: типы обратных связей, преимущество схем усилителей с обратными связями. Схемы усилителей на биполярных транзисторах: усилитель с общим коллектором, усилитель с общим эмиттером, усилитель с общей базой. Дифференциальный усилитель. Операционный усилитель: инвертирующий усилитель, неинвертирующий усилитель, сумматор, интегратор и гиратор. Источники вторичного электропитания: выпрямитель; фильтр; стабилизатор напряжения. **Электронные ключи.** Импульсный сигнал. Определение времени переходного процесса. Идеальный электронный ключ: ВАХ идеального ключа и нагрузочная прямая. Ключ на биполярном транзисторе: статический режим ключа на биполярном транзисторе; динамический режим ключа на биполярном транзисторе; ускоряющие элементы ключа на биполярном транзисторе. Ключи на полевых транзисторах: ключ на полевом транзисторе с резисторной нагрузкой; ключ на полевых транзисторах с динамической нагрузкой; ключ на комплементарных полевых транзисторах. **Базовые логические элементы.** Особенности схемного построения логических элементов: характерные разновидности схем логических элементов (схемы диодной логики, схемы диодно-транзисторной логики). Основные типы логических элементов: резисторно-транзисторная логика; диодно-транзисторная логика; транзисторно-транзисторная логика; расширение функциональных возможностей ТТЛ; эмиттерно-связанная логика; интегральная инжекционная логика; логические элементы на полевых транзисторах. Параметры интегральных логических элементов. **Конечные автоматы и комбинационные устройства.** Триггеры: асинхронный и синхронный RS-триггеры; двухступенчатый RS-триггер; триггер задержки (D-триггер) и JK-триггер. Регистры. Счетчики: счётчики с последовательным и параллельным вводом информации, кольцевые счетчики, счетчики с перекрестными связями. Комбинационные устройства: шифраторы, дешифраторы, мультиплексоры, демультиплексоры. **Устройства для получения импульсных сигналов.** Формирователи импульсов с элементами задержки и RC цепями. Формирователи коротких импульсов на собственных задержках и с RC цепочкой, интегральные компараторы, триггеры Шмитта. Ждущие и автоколебательные мультивибраторы на дискретных элементах. Ждущие и автоколебательные мультивибраторы на логических элементах и ОУ. Факторы, влияющие на стабильность параметров и методы стабилизации. Мультивибраторы в составе серий ИС. **Устройства аналого-цифрового преобразования.** ЦАП с весовыми сопротивлениями. ЦАП с резистивной матрицей R-2R, основные параметры. Интегральные ЦАП. Разновидности АЦП в интегральном исполнении. Быстродействующие параллельные АЦП, следящие АЦП, универсальные АЦП с поразрядным уравновешиванием, высокоточный АЦП с двойным интегрированием, АЦП косвенного преобразования. Параметры ЦАП и АЦП.

Рекомендуемый перечень лабораторных работ:

1. Исследование характеристик диодов.

2. Исследование характеристик транзисторов.

3. Исследование операционного усилителя и устройств на нем.

4. Исследование интегральных логических элементов.

5. Исследование ЦАП, АЦП.

Рекомендуемый перечень основной литературы:

1. Новожилов О.П. Электроника и схемотехника. В 2 т. Т.1.: Учебник. – М.: Юрайт, 2015. – 382 с.

2. Новожилов О.П. Электроника и схемотехника. В 2 т. Т.2.: Учебник. – М.: Юрайт, 2015. – 422 с.

3. Кучумов А.А., Кучумов А.И. Электроника и схемотехника: Учебное пособие. 5-е изд. – М.: Гелиос АРВ, 2017. – 368 с.

Перечень материально-технического обеспечения:

- лаборатория электроники и схемотехники, оснащенная учебно-лабораторными стендами, средствами для измерения и визуализации частотных и временных характеристик сигналов, средствами для измерения параметров электрических цепей, средствами генерирования сигналов;

- компьютерный класс, оснащенный рабочими местами на базе вычислительной техники с установленными программными средствами схемотехнического моделирования радиоэлектронных схем (Electronics Workbench версии не ниже 5 или аналогичными).

**Б.1.О.14. Модуль «Теория электросвязи» (Дисциплины «Теория электрических цепей», «Теория радиотехнических сигналов», «Теория электрической связи», «Теория информации и кодирования»)**

Коды формируемых компетенций: ОПК-11.

В результате изучения дисциплины студент должен

знать:

- устройство, принципы построения и работы, технические возможности и назначение, основные параметры и характеристики типовых электрических цепей;

- методы анализа электрических цепей при постоянных напряжениях, гармонических и произвольных воздействиях;

- основные математические модели, методы спектрального и корреляционного анализа сигналов, спектральные и корреляционные характеристики непрерывных и дискретных детерминированных сигналов;

- основные виды модуляции сигналов;

- способы представления сообщений, сигналов и помех, преобразования сигналов в каналах связи;

- основы оптимального приема сигналов в присутствии помех и типовые схемы оптимальных приемников;

- основные понятия теории информации;

- основные коды источников информации и помехоустойчивые коды, основные параметры и способы представления помехоустойчивых кодов;

уметь:

- рассчитывать основные параметры типовых электрических цепей в стационарных и переходных режимах процессов в них;

- производить оценку и измерение отдельных характеристик типовых электрических цепей;

- рассчитывать спектральные и корреляционные характеристики типовых детерминированных сигналов;

- выбирать статистические модели сигналов и помех, типовые схемы оптимальных приемников и оценивать помехоустойчивость оптимального приема типовых сигналов на фоне помех;

- рассчитывать параметры помехоустойчивых кодов;

- применять базовые способы кодирования и декодирования типовых помехоустойчивых кодов и кодов источников информации.

Примерное распределение часов: трудоемкость дисциплины 20 з.е., 720 час.

Форма контроля: 4 экзамена.

Содержание дисциплины:

**Основные понятия и законы теории электрических цепей.** Цепи постоянного и переменного тока. Схема цепи и топологические понятия. Электрические цепи с двухполюсными и многополюсными элементами. Пассивные элементы и схемы замещения. Источники тока и напряжения, зависимые источники. Временное и спектральное представления сигналов. Законы Ома, Кирхгофа, Джоуля-Ленца, электромагнитной индукции. Колебания в электрических цепях. Переходные и установившиеся процессы. Линейные цепи, принцип суперпозиции, параметрические и нелинейные цепи. Задачи анализа и синтеза электрических цепей. **Электрические цепи постоянного тока и методы их анализа.** Электрическая цепь с источниками постоянного напряжения и тока. Генераторы напряжения и тока. Согласование источников с нагрузкой. Согласование по напряжению, по току, по мощности. Методы расчета простых и сложных электрических цепей. Методы токов ветвей, контурных токов и узловых потенциалов. Метод эквивалентного генератора. Применение теоремы взаимности для расчета сложных цепей. **Электрические цепи при гармонических воздействиях и методы их анализа.** Мгновенное значение, амплитуда, частота, фаза, среднее и эффективное значение гармонического тока (напряжения). Временные и векторные диаграммы напряжений и токов для пассивных элементов цепи. Основы символического метода анализа электрических цепей. Комплексные амплитуды токов и напряжений. Мгновенное значение гармонического сигнала в комплексной форме. Основные законы электрических цепей в комплексной форме. Комплексное сопротивление и комплексная проводимость пассивных двухполюсников. Поглощаемая мощность и запасаемая энергия в пассивных двухполюсниках. Мощность переменного тока в комплексной форме. Последовательное и параллельное соединение пассивных двухполюсников. Колебательный контур. Резонанс токов и напряжений. Расчет сложных электрических цепей символическим методом: метод контурных токов и метод узловых потенциалов. **Трехфазные электрические цепи**. Трехфазные электрические цепи, соединение фаз цепи. Симметричные и несимметричные трехфазные цепи. Основные расчетные соотношения, энергетические соотношения для трехфазной электрической цепи. **Методы анализа линейных цепей при произвольных детерминированных воздействиях.** Временной и спектральный подходы к анализу электрических цепей при произвольных воздействиях. Временной метод анализа четырехполюсников. Импульсная и переходная характеристики четырехполюсников. Интеграл наложений (интеграл Дюамеля) и его применение при анализе цепей. Спектральный метод анализа четырехполюсников; метод интеграла Фурье. Операторный метод анализа электрических цепей. Законы Ома и Кирхгофа в операторной форме. Операторные сопротивления и проводимости. Передаточная функция цепи. **Частотные характеристики линейных цепей.** Комплексные частотные характеристики линейных электрических цепей. Амплитудно-частотные и фазо-частотные характеристики. Последовательный и параллельный колебательные контуры. Резонанс токов и напряжений. Избирательность и полоса пропускания одиночных контуров. Связанные колебательные контуры. Колебательные цепи в приемо-передающей аппаратуре. Линейные цепи с переменными параметрами. **Основы теории четырехполюсников.** Четырехполюсники, их определение и классификация. Системы уравнений и параметры четырехполюсников. Взаимосвязь параметров четырехполюсников. Эквивалентные схемы четырехполюсника. Способы соединений четырехполюсников. Сложные четырехполюсники, основные типы простых четырехполюсников. Четырехполюсники с обратной связью. Передаточная функция четырехполюсника. **Электрические фильтры.** Электрические фильтры, их определение и классификация. Типы электрических *LC*-фильтров. Основные соотношения и характеристики. Специальные типы электрических фильтров: мостовые, безындукционные, пьезоэлектрические, магнитострикционные фильтры. Области применения электрических фильтров. **Линейные усилительные устройства.** Определение, классификация и основные показатели усилителей. Три схемы усилителей на транзисторах, их сравнительный анализ. Резистивные и резонансные усилители, их амплитудно-частотные характеристики. Применение обратной связи в усилителях. Области применения линейных усилительных устройств. **Цепи с распределенными параметрами.** Общие сведения о длинных линиях. Телеграфные уравнения. Решение телеграфных уравнений в частотной области. Бегущие волны в длинной линии. Волновые параметры длинной линии с потерями и без потерь. Коэффициент отражения. Стоячие и смешанные волны в линии, условия их образования. Входное сопротивление линии с комплексной нагрузкой. Аналогия между уравнениями линии с распределенными параметрами и уравнениями четырехполюсника. Свойства разомкнутого и замкнутого на конце отрезка линии без потерь. Линия без потерь, нагруженная на активный, реактивный, комплексный импеданс. Применение длинных линий на практике. **Введение в теорию нелинейных цепей.** Введение в теорию нелинейных цепей. Некоторые характеристики нелинейных элементов. Аппроксимация характеристик нелинейных элементов. Нелинейное преобразование формы сигнала. Нелинейное преобразование спектра сигнала. Безынерционное нелинейное преобразование суммы гармонических колебаний. Комбинационные частоты. Эффект интермодуляции. Совместное воздействие на нелинейный элемент сигналов большой и малой амплитуд. **Нелинейное усиление и умножение частоты электрических колебаний.** Нелинейное резонансное усиление. Квазилинейный метод анализа нелинейного усилителя. Понятие средней крутизны усилительного элемента и колебательной характеристики нелинейного резонансного усилителя. КПД нелинейного усилителя. Умножение частоты и усиление гармоник. Амплитудный ограничитель. Области применения нелинейных резонансных усилителей, умножителей частоты и амплитудных ограничителей. **Генерирование электрических колебаний.** Устойчивость активных электрических цепей. Критерии устойчивости. Механизм возбуждения колебаний в системе. Основные элементы *LC*-автогенератора. Условия самовозбуждения. Стационарный режим работы автогенератора. Баланс фаз и баланс амплитуд. Определение амплитуды и частоты установившихся колебаний. Мягкий и жесткий режимы самовозбуждения. Способы стабилизации частоты автогенераторов. Особенности построения RC-автогенераторов. Области применения автогенераторов. **Общие представления о модуляции, детектировании и преобразовании частоты колебаний.** Общие сведения о процессах модуляции и детектирования. Понятия о методах амплитудной, частотной и фазовой модуляции. Особенности осуществления однополосной модуляции. Понятия о детектировании АМ-колебаний, однополосном и гетеродинном детектировании. Особенности построения детекторов ЧМ- и ФМ-колебаний. Общие сведения о процессе преобразования частоты. Преобразование частоты в нелинейных и параметрических цепях. Особенности построения и принципы работы диодных и балансных преобразователей частоты. Области применения модуляционных устройств, детекторов и преобразователей частоты. **Элементы синтеза электрических цепей.** Задача синтеза электрических цепей. Характеристики (функции) цепей и связь между ними. Свойства обобщенных входных функций. Критерии физической осуществимости двухполюсника. Синтез двухполюсника по заданной входной функции. Общие представления о синтезе четырехполюсников. **Теория радиотехнических сигналов. Основные понятия и определения:** первичные сигналы, видеосигналы, радиосигналы, помехи и искажения. Математические модели и классификация радиотехнических сигналов. **Методы представления сигналов.** Динамическое представление сигналов посредством функций включения и дельта-функций, понятие обобщенных функций. Векторное представление сигналов: Евклидово и Гильбертово пространства сигналов, классификация сигналов по коэффициенту корреляции, оценка потенциальной помехоустойчивости сигналов по расстоянию между концами сигнальных векторов. Энергия и мощность сигналов. Ортогональные сигналы. Описание сигналов временными функциями: действительные и комплексные сигналы. Понятие аналитического и сопряженного сигналов: математическая модель, энергия и взаимосвязь их спектров. **Спектральный анализ периодических сигналов:** тригонометрический ряд Фурье, комплексный ряд Фурье, спектры типовых периодических сигналов. **Спектральный анализ непериодических сигналов:** прямое и обратное преобразования Фурье, физический смысл спектрального представления сигналов, спектры типовых одиночных импульсов, взаимосвязь спектров одиночного импульса и периодической последовательности импульсов. Основные свойства преобразований Фурье и их использование при определении спектров сигналов. Спектры типовых неинтегрируемых сигналов. Текущий и мгновенный спектры сигнала. Энергетический спектр сигнала: физический смысл, распределение мощности в спектре сигнала, скорость убывания спектра, ширина спектра, необходимая и занимаемая полосы частот, соотношение между длительностью сигнала и шириной его спектра. **Корреляционные функции сигналов.** Виды корреляционных функций сигналов. Автокорреляционные функции периодического и непериодического сигналов, их взаимосвязь с соответствующими энергетическими спектрами. Интервал корреляции и эффективная ширина спектра сигнала. Взаимная корреляционная функция двух сигналов, ее свойства и взаимосвязь с взаимным энергетическим спектром этих сигналов. **Узкополосные сигналы. Импульсные и цифровые видеосигналы. Аналоговые радиосигналы. Импульсные и цифровые радиосигналы. Широкополосные сигналы:** сигналы с расширением полосы и сигналы с расширением спектра сигналов, когерентные и некогерентные сложные сигналы, сигналы с гармонической и с дискретной несущей, кодовые псевдослучайные последовательности и шумоподобные сигналы. Шумоподобные двоичные ФМн-сигналы. Системы фазоманипулированных сигналов: полный код системы сигналов, кодовые последовательности Уолша, кодовые последовательности Велти, производные, сегментные и циклические системы сигналов, объем больших систем сигналов, оценки апериодических взаимно-корреляционных функций. **Принципы построения систем связи:** основные понятия, виды систем связи, помехоустойчивость, основные характеристики и показатели эффективности. Структурная схема системы связи: состав и назначение элементов, основные преобразования сообщений и сигналов (дискретизация, квантование, кодирование и декодирование, манипуляция, модуляция и детектирование), проблема электромагнитной совместимости. **Дискретизация непрерывных первичных сигналов:** теорема Котельникова, оценка погрешности дискретизации при регулярном опросе, использование теоремы Котельникова для выбора частоты опроса реальных первичных сигналов с неограниченным спектром, восстановление непрерывных первичных сигналов по выборкам (интерполяция и экстраполяция). Квантование и кодирование значений выборок первичных сигналов: способы квантования, оценка погрешности равномерного квантования, виды представления непрерывных первичных сигналов (аналоговое, дискретно-непрерывное, непрерывно-квантованное, дискретно-квантованное, цифровое представление), кодирование значений квантованных выборок (импульсно-кодовая модуляция (ИКМ), дифференциальная ИКМ, дельта-модуляция, компадирование). **Прохождение сигналов через каналы связи:** преобразование детерминированных и случайных сигналов в детерминированных линейных и нелинейных каналах, прохождение сигналов через случайные каналы связи, нормализация случайных процессов линейными инерционными системами. Преобразование колебаний в параметрических и нелинейных цепях. Основы теории линейного разделения сигналов: условия независимости и ортогональности сигналов. **Методы уплотнения каналов:** частотное, фазовое, временное, кодовое и комбинационное уплотнение каналов, пропускная способность многоканальных систем связи, влияние на нее взаимных помех. **Модуляция и детектирование аналоговых сигналов:** методы аналоговой модуляции, формирование и детектирование аналоговых сигналов с амплитудной, балансной, однополосной, фазовой и частотной модуляцией, методы аналого-импульсной модуляции, формирование и детектирование аналоговых импульсных сигналов с амплитудно-импульсной, фазо-импульсной и широтно-импульсной модуляцией. **Модуляция и детектирование цифровых сигналов:** методы кодо-импульсной модуляции, формирование и детектирование цифровых сигналов с амплитудной, фазовой, относительной фазовой и частотной манипуляцией. **Задачи синтеза оптимальных демодуляторов:** апостериорные вероятности и апостериорные плотности вероятности, функции и функционалы правдоподобия, отношение правдоподобия, функция взаимной корреляции, критерии оптимального приема. Особенности приема дискретных и непрерывных сообщений: алгоритмы оптимального приема по критериям идеального наблюдателя и максимального правдоподобия. **Помехоустойчивость систем передачи дискретных и непрерывных сообщений.** Помехоустойчивость оптимального когерентного приема: вероятность ошибки при приеме полностью известных цифровых сигналов с амплитудной, фазовой, относительной фазовой и частотной манипуляцией, оценка энергетического проигрыша при неточной синхронизации. Помехоустойчивость оптимального некогерентного приема: вероятность ошибки при приеме ортогональных сигналов с неизвестной случайной фазой, цифровых сигналов с амплитудной, фазовой, относительной фазовой и частотной манипуляцией. Оптимальный прием непрерывных сообщений: геометрическая модель системы передачи непрерывных сообщений, линия сигналов, влияние помех, коэффициент растяжения сигнала, пороговый эффект, нормальные и аномальные погрешности, оптимальная оценка отдельных параметров и оптимальная демодуляция непрерывных сигналов, оптимальный прием аналоговых радиосигналов с амплитудной и угловой модуляцией. Фильтрация сигналов: оптимальная линейная фильтрация непрерывных случайных сигналов, фильтр Колмогорова-Винера, фильтр Калмана, оценка погрешности линейной фильтрации, минимизация дисперсии погрешности, согласованные и квазиоптимальные линейные фильтры, нелинейная фильтрация аналоговых и двоичных сигналов. Помехоустойчивость оптимального приема аналоговых радиосигналов с амплитудной и угловой модуляцией: помехоустойчивость оптимального синхронного фазового детектора (СФД) и квазиоптимального СФД, сравнение различных методов приема ЧМ сигналов. Помехоустойчивость оптимального приема аналоговых импульсных радиосигналов: оценка вероятности появления аномальной погрешности и дисперсии нормальной погрешности при оптимальном приеме сигналов АИМ-ЧМ и ФИМ-АМ, оптимизация их параметров. Эффективность систем связи: диаграмма и предельная взаимосвязь показателей энергетической и спектральной эффективности систем связи, критерии сравнения и оптимальности систем связи по показателям энергетической и спектральной эффективности. Сравнение систем связи: по помехоустойчивости, по необходимой и занимаемой полосе частот, по показателям энергетической и спектральной эффективности, оптимизация параметров систем связи. Системные методы повышения достоверности передачи сообщений: системы с повторением сообщений, системы с прерыванием, системы с обратной связью, системы с помехоустойчивым кодированием. **Теория информации.** Основные понятия, определения теории информации. Информация, сообщение, сигнал. Обобщенные характеристики сигналов и информационных каналов. Понятие о мерах информации: количество информации и неопределенность, энтропия как мера неопределенности. Производительность источника, скорость передачи информации и пропускная способность канала. Дискретные и непрерывные ансамбли и источники сообщений. Количество информации в дискретных сообщениях. Энтропия источника дискретных сообщений. Свойства энтропии. Производительность источника дискретных сообщений. Взаимная информация дискретных ансамблей, энтропия сложных сообщений, совместная и условная энтропия. Свойства взаимной информации и энтропии сложных сообщений. Избыточность источника дискретных сообщений. Количество информации в непрерывных сообщениях. Дифференциальная энтропия. Взаимная информация для непрерывных ансамблей. Эпсилон-энтропия и эпсилон-производительность источника непрерывных сообщений. Избыточность источника непрерывных стационарных сообщений. **Кодирование источника дискретных сообщений.** Теорема оптимального кодирования. Равномерное кодирование. Производительность источника дискретных сообщений при равномерном кодировании. Неравномерное кодирование. Оптимальные статистические коды. Код Шеннона-Фано. Код Хаффмена. Кодирование источника дискретных сообщений при неизвестной статистике. Алгоритмы кодирования источника, применяемые в архиваторах. Задача кодирования источника непрерывных сообщений. Регулярная и адаптивная дискретизация. Равномерное и неравномерное квантование, квантование с компадированием. Цифровое кодирование непрерывных сообщений: импульсно-кодовая модуляция. Безизбыточные двоичные коды: двоичный натуральный код, симметричный двоично-числовой код, код Грея. Цифровое кодирование непрерывных сообщений с предсказанием: дифференциальная импульсно-кодовая модуляция и дельта-модуляция. Особенности сжатия речи. Особенности сжатия неподвижных и подвижных изображений. **Информационные модели каналов:** дискретные, дискретно-непрерывные и непрерывные каналы. Скорость передачи информации и пропускная способность дискретного канала без помех. Скорость передачи информации и пропускная способность дискретного канала с помехами. Скорость передачи информации и пропускная способность непрерывного канала с аддитивным шумом. Основная теорема кодирования для канала без помех и для канала с помехами. Кодирование формы первичных сигналов: код с возвратом к нулю, код без возврата к нулю, биимпульсный (манчестерский) код. Спектральное кодирование: квазитроичный (биполярный) код, код с чередованием полярности. Логическое кодирование: код высокой плотности КВП-3, скремблирование. Линейное кодирование: код 4В3Т, код 2B1Q.Перекодирование формы сигналов на выходе канала при использовании методов частичного отклика: дуобинарный метод, кодирование по методу Лендера. **Основные понятия, определения теории помехоустойчивого кодирования.** Способы представления кодовой комбинации, кодовое расстояние и вес кодовой комбинации. Скорость, избыточность и корректирующая способность кода. Сущность помехоустойчивого кодирования. Типы, обозначения и классификация помехоустойчивых кодов. Коды для каналов с нормальным белым шумом и для каналов с пакетированием ошибок. Связь корректирующей способности и скорости кода. Вероятность ошибки на символ и на бит при использовании помехоустойчивого кодирования. Выигрыш от кодирования. Выбор помехоустойчивого кода. **Блочные коды.** Основные параметры блочных кодов. Порождающая и проверочная матрицы. Способы задания блочных кодов. Способы кодирования. Способы декодирования. Синдромное декодирование блочных кодов. Коды Хемминга. Модификация кодов Хемминга. Вероятность ошибки на символ и на бит, выигрыш от кодирования при использовании кодов Хемминга. Основные параметры циклических кодов. Порождающий и проверочный многочлены. Способы задания циклических кодов. Задание циклического кода с помощью минимальных многочленов. Наиболее известные циклические коды. Модификация циклических кодов. Способы кодирования. Аппаратная реализация кодеров. Способы декодирования. Мажоритарное декодирование: система разделенных проверок, система квазиразделенных проверок. Аппаратная реализация декодеров. Метод максимального правдоподобия. Декодирование с «жестким» и «мягким» решением. Синдромное декодирование циклических кодов. Алгоритм Берлекемпа-Месси. Качество и вычислительная сложность декодирования. Коды БЧХ. Код Голея. Коды Рида-Соломона. Вероятность ошибки на символ и на бит, выигрыш от кодирования при использовании кодов БЧХ, кода Голея и кодов Рида-Соломона. Методика выбора кода БЧХ с заданной корректирующей способностью. **Сверточные коды.** Основные параметры сверточных кодов. Способы задания сверточных кодов: порождающая матрица, представление связей, полиномиальное представление и импульсный отклик сверточного кодера. Древовидная диаграмма Диаграмма состояний. Решетчатая диаграмма. Наиболее известные сверточные коды. Способы кодирования. Способы декодирования. Алгоритм максимального правдоподобия. Алгоритм Витерби. Декодирование с «жестким» и «мягким» решением. Последовательное декодирования. Алгоритм Фано. Декодирование с обратной связью. Сравнительная характеристика алгоритмов декодирования. Вероятность ошибки на символ и на бит, выигрыш от кодирования при использовании сверточных кодов.

Рекомендуемый перечень лабораторных работ:

1. Исследование *RC* - и *RL*-цепей.

2. Исследование последовательного и параллельного колебательных контуров или системы двух связанных колебательных контуров.

3. Исследование четырехполюсников.

4. Исследование электрических фильтров.

5. Исследование резистивного или резонансного линейного усилителя.

6. Исследование нелинейного резонансного усилителя и умножителя частоты.

7. Исследование процесса генерирования гармонических колебаний.

8. Исследование процесса амплитудной (частотной) модуляции, процесса детектирования АМ колебаний или процесса преобразования частоты.

9. Исследование спектров сигналов.

10. Исследование узкополосных сигналов.

11. Исследование методов модуляции сигналов.

12. Преобразование сигналов в каналах связи.

13. Модуляция и детектирование сигналов.

14. Оценка помехоустойчивости цифровых радиосигналов.

15. Оценка помехоустойчивости аналоговых радиосигналов.

16. Исследование корректирующей способности блочных кодов.

17. Исследование корректирующей способности циклических кодов.

18. Исследование корректирующей способности перемежителей.

19. Исследование корректирующей способности сверточных кодов.

Рекомендуемый перечень основной литературы:

1. Атабеков Г.И. Теоретические основы электротехники. Линейные электрические цепи: Учебное пособие для вузов. 8-е издание, стереотипное. – СПб: Лань, 2010.

2. Гоноровский И. С. Радиотехнические цепи и сигналы: Учебное пособие для вузов. – М.: Дрофа, 2006. – 719 с.

3. Запасный А. И. Основы теории цепей: Учебное пособие. – М.: РИОР, 2010.–336 с.

4. Баскаков С.И. Радиотехнические цепи и сигналы. – М.: «Ленанд», 2016. – 528 с.

5. Клюев Л.Л. Теория электрической связи. – М.: «Инфра-М», 2016. – 448 с.

6. Панин В.В. Основы теории информации. – М: «Бином», 2014. – 440 с.

7. Чечета С.И. Введение в дискретную теорию информации и кодирования. – М.: «МЦНМО», 2011. – 224 с.

8. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. – М.: «Вильямс», 2016 – 1104 с.

Перечень материально-технического обеспечения:

- лаборатория электроники и схемотехники, оснащенная учебно-лабораторными стендами, средствами для измерения и визуализации частотных и временных характеристик сигналов, средствами для измерения параметров электрических цепей, средствами генерирования сигналов;

- компьютерный класс, оснащенный рабочими местами на базе вычислительной техники с установленным программным обеспечением, предназначенным для математических вычислений и моделирования (MATLAB R2014 и выше или аналогичное).

**Б.1.О.15. Дисциплина «Антенны и распространение радиоволн»**

Коды формируемых компетенций: ОПК-11.

В результате изучения дисциплины студент должен

знать:

- физические основы излучения и распространения радиоволн в различных средах, а также особенности распространения радиоволн различных диапазонов частот;

- основные типы, принципы действия, характеристики и особенности антенн, линий передачи, элементов волноводной и фидерной техники, методы и приемы расчета их характеристик;

уметь:

- рассчитывать параметры типовых трасс распространения радиоволн;

- рассчитывать характеристики типовых антенн, линий питания и отдельных устройств СВЧ.

Примерное распределение часов: трудоемкость дисциплины 4 з.е., 144 час.

Форма контроля: зачет с оценкой.

Содержание дисциплины:

**Система уравнений электродинамики.** Интегральная и дифференциальная формы уравнений Максвелла с токами и зарядами. Локальная форма закона сохранения электрического заряда. Магнитные токи и заряды. Перестановочная двойственность. Скалярный и векторный потенциалы электромагнитного поля, их неоднозначность. Градиентная (калибровочная) инвариантность. Электрический и магнитный векторы Герца. Уравнения для векторов Герца. Решение неоднородного волнового уравнения в виде запаздывающих потенциалов. **Излучение электромагнитных волн элементарными излучателями.** Сторонние токи и заряды. Локализованный в пространстве излучатель. Поля элементарных электрического и магнитного диполей в ближней и волновой зоне. **Электромагнитные волны в различных средах.** Классификация сред. Электрическая поляризация и намагниченность. Электромагнитные волны в прозрачных средах. Коэффициент преломления. Понятие о частотной дисперсии. Фазовая и групповая скорости электромагнитных волн. Граничные условия для векторов поля на границе раздела двух сред. Отражение и преломление электромагнитных волн на плоской границе. Формулы Френеля. Особенности пространственной структуры электромагнитного поля при полном отражении. Электромагнитные волны в средах с малой проводимостью. Комплексный волновой вектор. Коэффициент поглощения. Комплексная диэлектрическая проницаемость. Скин-эффект в металлах. Граничные условия Леонтовича на границе раздела диэлектрик-металл. **Основы теории направляющих систем и резонаторов.** Открытые и закрытые направляющие системы. Уравнения для электромагнитного поля в направляющей системе. Классификация направляемых волн. Критическая длина волны. Фазовая скорость. Характеристическое сопротивление. Прямоугольный и круглый волноводы. Коаксиальная линия. Структура волн, основные параметры и характеристики. Затухание волн в волноводах. Прямоугольный резонатор. Моды колебаний. Добротность. **Распространение радиоволн.** Распространение радиоволн в свободном пространстве. Формула идеальной радиопередачи. Поле источника, расположенного над плоской идеально проводящей поверхностью. Множитель интерференции и его особенности для волн горизонтальной и вертикальной поляризации. Квадратичная формула Введенского. Распространение радиоволн над реальной земной поверхностью. Критерий Рэлея шероховатости отражающей поверхности. Диффузное отражение. Влияние сферичности земной поверхности. Дальность прямой видимости. Диэлектрическая проницаемость и показатель преломления тропосферы, его зависимость от высоты. Рассеяние и поглощение радиоволн в тропосфере. Дальнее тропосферное распространение. Ионосфера и ионосферная плазма. Преломление, отражение и поглощение радиоволн в ионосфере. Условие отражения. Предельная и критическая частоты. Дальность скачка. Влияние магнитного поля Земли на распространение радиоволн. Классификации диапазонов частот. Особенности распространения длинных и средних волн. Особенности распространения коротких волн. Поверхностные и пространственные волны. Зона молчания. Многоскачковое распространение радиоволн. Особенности распространения метровых, дециметровых и сантиметровых волн в пределах прямой видимости, за её пределами, на линиях космической связи. Распространение волн оптического диапазона. **Общая теория передающих антенн.** Общая классификация антенн. Поле системы токов. Зоны излучения. Особенности полей в дальней зоне. Диаграмма направленности. Коэффициент направленного действия и коэффициент усиления. Поляризационные характеристики. Действующая длина и высота антенны. Эффективная площадь. Мощность и сопротивление излучения, входное сопротивление. Рабочий диапазон частот. Классификация антенн по полосе рабочих частот. **Элементарные антенны.** Поле провода со стоячей волной тока. Симметричные и несимметричные вибраторы. Полуволновой вибратор. Широкополосные вибраторы. Поле провода с бегущей волной тока. V-образные и ромбические антенны. Щелевые антенны. Турникетные антенны. **Общая теория приемных антенн.** Обратимость передающих и приемных антенн. Применение принципа взаимности для анализа приемной антенны. ЭДС на выходе и эквивалентная схема приёмной антенны. Идентичность параметров в режиме передачи и приема. Мощность, передаваемая в нагрузку. Условие согласования антенны и её нагрузки. Рамочные и ферритовые приемные антенны. **Направленные свойства системы излучателей.** Диаграмма направленности системы излучателей. Теорема умножения и множитель решетки. Основные типы антенных решеток. Множитель и режимы работы линейной эквидистантной решетки. **Многоэлементные антенны.** Двухвибраторная антенна. Антенна типа «волновой канал». Синфазная горизонтальная диапазонная антенна. Вибраторные антенны бегущей волны. Спиральные антенны. Логопериодические антенны. **Антенны с излучающим раскрывом.** Принцип действия типичной антенны СВЧ, методы её анализа. Апертурный и токовый методы. Формула Кирхгофа и ее применение. Диаграмма направленности, коэффициент направленного действия и коэффициент использования площади плоского синфазного раскрыва (прямоугольного и круглого). Влияние амплитудных распределений и фазовых ошибок на диаграмму направленности и КНД. Рупорные антенны. Оптимальные рупоры. Линзовые антенны Зеркальные антенны. **Антенны бегущей волны и микрополосковые антенны.** Антенны поверхностных волн, их разновидности, принцип действия и основные характеристики. Миниатюризация современных антенн. Антенны в печатном исполнении. Микрополосковые антенны. Антенны Вивальди. **Высокочастотное питание антенн. Согласование и симметрирование.** Типы и параметры основных линий передачи. Проблема согласования и симметрирования линии питания и антенны. Основные схемы симметрирующих и согласующих устройств. Элементы волноводной и фидерной техники. Ферритовые устройства.

Рекомендуемый перечень лабораторных работ:

1. Измерение коэффициента усиления антенны.

2. Измерение диаграммы направленности антенны в режиме передачи.

3. Исследование симметричных вибраторов.

4. Исследование антенны типа «волновой канал».

5. Исследование влияния амплитудных и фазовых распределений   
на направленные свойства антенны.

Рекомендуемый перечень основной литературы:

1. Сомов А.М., Старостин В.В., Бенеславский С.Д. Электродинамика: Учебное пособие для вузов. / Под ред. А.М. Сомова. – М.: Горячая линия–Телеком, 2011. – 200 с.: ил.

2. Распространение радиоволн: Учебное пособие для вузов. / А.М. Сомов, В.В. Старостин. – М.: Гелиос АРВ, 2010. – 264 с.

3. Сомов А.М., Старостин В.В., Кабетов Р.В. Антенно-фидерные устройства: Учебное пособие для вузов. / Под ред. А.М. Сомова. – М.: Горячая линия–Телеком, 2011. – 404 с.: ил.

Перечень материально-технического обеспечения:

- лаборатория, оборудованная комплектами лабораторных стендов   
и необходимыми измерительными приборами (генераторы УВЧ-СВЧ колебаний, селективные вольтметры или анализаторы спектра, два комплекта измерительных антенн);

- компьютерный класс, оснащенный рабочими местами на базе вычислительной техники с установленным программным обеспечением, предназначенным для моделирования электродинамических процессов и расчета антенн (MMANA-GAL, CST Studio Suite, ANSYS Electromagnetic Suite или аналогичные).

**Б.1.О.16. Дисциплина «Цифровая обработка сигналов»**

Коды формируемых компетенций: ОПК-11.

В результате изучения дисциплины студент должен

знать:

- дискретные и цифровые сигналы и системы, способы их представления   
и описания, основные методы анализа дискретных сигналов и систем;

- методы проектирования цифровых фильтров.

уметь:

- применять методы анализа и синтеза цифровых сигналов и систем для решения задач профессиональной деятельности.

Примерное распределение часов: трудоемкость дисциплины 4 з.е., 144 час.

Форма контроля: зачет с оценкой.

Содержание дисциплины:

**Дискретные сигналы и системы.** Дискретные системы и их типы. Линейные инвариантные к сдвигу системы. Физическая реализуемость и устойчивость дискретных систем. Свойства линейных инвариантных к сдвигу систем. **Преобразование Фурье.** Преобразование Фурье дискретных сигналов. Дискретное преобразование Фурье (ДПФ). Свойства дискретного преобразования Фурье. Искажения сигналов при ДПФ. Быстрое преобразование Фурье. **Z-преобразование.** Z-преобразования некоторых последовательностей. Свойства Z-преобразования: линейность, задержка, свертка последовательностей, перемножение последовательностей, задержка физически реализуемых последовательностей. **Цифровая фильтрация.** Системы, описываемые разностными уравнениями. Импульсная характеристика. Передаточная функция. Частотная характеристика. Связь между характеристиками. Фильтры с конечной и бесконечной импульсной характеристикой. Структурные схемы фильтров. Устойчивость цифровых фильтров. Применение Z-преобразования в задачах описания и анализа дискретных систем. **Дискретное преобразование Гильберта и его свойства.** Идеальный дискретный дифференцирующий фильтр. **Методы синтеза цифровых фильтров.** Формулировка задачи синтеза цифрового фильтра. Требование устойчивости, линейности фазовой характеристики. Методы синтеза КИХ-фильтров. Синтез фильтров по методу окна. Весовые функции в методе окна. Фильтры на основе частотной выборки. Синтез оптимального фильтра. Основные методы синтеза БИХ-фильтров. Аналоговые фильтры, их типы и характеристики. Методы аппроксимации аналоговых фильтров. **Приложения цифровой обработки сигналов.** Изменение частоты дискретизации сигнала. Постановка задачи интерполяции. Способы интерполяция. Множественная фильтрация. Модуляция и демодуляция сигналов. Применение вейвлетов в задачах шумоочистки и сжатия сигналов.

Рекомендуемый перечень лабораторных работ:

1. Исследование свойств спектра дискретного сигнала.

2. Расчет и исследование цифровых фильтров.

3. Изменение частоты дискретизации сигнала, выбеливание шума.

Рекомендуемый перечень основной литературы:

1. Оппенгейм А.В., Шафер Р.В. Цифровая обработка сигналов. – М.: Техносфера, 2010. – 855 с.

2. Айчифер Э., Джервис Б. Цифровая обработка сигналов: практический подход, 2-е издание. Пер. с англ. – М.: Издательский дом «Вильяме», 2015. – 992 с.

3. Штарк Г.Г. Применение вейвлетов для ЦОС. – М.: Техносфера, 2007. –   
192 с.

4. Сергиенко А. Б. Цифровая обработка сигналов. СПб: ПИТЕР, 2007. – 750 с.

5. Лайонс Р. Цифровая обработка сигналов. Пер. с англ. – М.: Бином, 2006. – 654 с.

Перечень материально-технического обеспечения:

лаборатория (класс) цифровой обработки сигналов, оснащенный рабочими местами на базе вычислительной техники с установленным программным обеспечением для цифровой обработки сигналов (Adobe Audition (Cool Edit), MATLAB, QED или их аналогами).

**Б.1.О.17. Дисциплина «Языки программирования»**

Коды формируемых компетенций: ОПК-7.

В результате изучения дисциплины студент должен

знать:

- представления данных в памяти компьютера;

- основные конструкции и библиотеки языка программирования;

- принципы построения программ в процедурно-ориентированной и объектно-ориентированной парадигмах;

уметь:

- реализовывать алгоритмы на языке программирования;

- работать с интегрированной средой разработки программного обеспечения;

- использовать сторонние программные библиотеки;

владеть:

- навыками разработки и тестирования программ по поставленной спецификации.

Примерное распределение часов: трудоемкость дисциплины 10 з.е., 360 час.

Форма контроля: 2 зачета, экзамен.

Содержание дисциплины:

**Информация, информатика, принципы построения компьютера.** Подходы к определению понятий «информация» и «информатика». Виды и формы информации. Принципы построения компьютера. Архитектура фон Неймана. Цикл формирования и исполнения команд компьютера. Файловые системы. Работа в командной строке. **Язык программирования С/С++.** Характеристика языка, стандарты, этапы создания исполняемого файла. Инструментальные средства разработки программного обеспечения на языке С/С++. Базовые конструкции языка С/С++. Алфавит, идентификаторы, служебные слова, константы. **Системы счисления.** Целочисленные и вещественные типы данных, представление целых и вещественных чисел в компьютере. Представление символьной и строковой информации в компьютере и в С++. **Операции, выражения в языке С/С++.** Операторы последовательного выполнения, операторы выбора, операторы цикла, операторы передачи управления. **Основы структурного программирования.** Указатели и ссылки. Операции с указателями. Организация работы с динамической памятью. Массивы. Одномерные массивы. Двумерные массивы. Динамические массивы. Строки. Структуры, объединения, битовые поля. Перечислимые типы. Переопределение типов. Форматируемый ввод-вывод данных. Работа с файлами. Функции. Определение, описание и вызов функции. Способы передачи параметров в функцию. Рекурсивные функции. Указатели на функции. Встраиваемые функции. Параметры по умолчанию. Параметры функции main. Функции с переменным числом параметров. Перегрузка функций. Шаблоны функций. Классы памяти. Область видимости, действия, время жизни переменной. Пространства имен. Пространство имен std. Препроцессорные средства. Директивы и стадии препроцессорной обработки. Условная компиляция. Макроподстановки. Операции с разрядами. Поразрядные логические операции и операции сдвига**. Основы объектно-ориентированного программирования.** Понятия абстракции, абстрактного типа данных. Основные понятия объектно-ориентированного программирования (ООП). Инкапсуляция, наследование и полиморфизм. Классы. Понятие класса. Доступ к компонентам класса. Конструкторы и деструкторы. Поля и методы класса. Указатель this. Статические компоненты класса. Дружественные функции и классы. Перегрузка операторов. Локальные классы. Наследование. Полиморфизм. Виртуальные функции. Абстрактные классы. Потоковые средства ввода/вывода данных. Иерархия классов потоков в языке C++. Форматированный ввод/вывод. Создание собственных манипуляторов. Файловый ввод/вывод. Исключительные ситуации. Основные понятия. Механизм обработки исключений. Классы исключений. Шаблоны классов. Определение шаблона классов, типы параметров шаблона. Инстанцирование шаблона. Специализация шаблона. **Стандартная библиотека шаблонов STL.** Общие принципы функционирования STL. Контейнеры. Итераторы. Алгоритмы. Адаптеры. Функторы. Строки в языке С++. Библиотечный класс string.

Рекомендуемый перечень лабораторных работ:

1. Представление числовых данных в памяти компьютера.

2. Форматированный ввод-вывод данных.

3. Потоковые средства ввода-вывода данных.

Рекомендуемый перечень основной литературы:

1. Грошев А.С., Закляков П.В. Информатика: учеб. для вузов – 3-е изд., перераб. и доп. – М.: ДМК Пресс, 2016. – 588 с.: цв. ил.

2. Джосаттис Н.М. Стандартная библиотека С++: справочное руководство, 2-е изд. – М.: ООО «И.Д. Вильямс», 2014. – 1136 с.

4. Павловская Т.А. С/С++. Структурное и объектно-ориентированное программирование. Учебник для вузов. – СПб.: Питер, 2015. – 496 с.

5. Шилдт Г. C++: базовый курс: Пер. с англ. – М.: Издательский дом «Вильямс», 2016. – 624 с.

Перечень материально-технического обеспечения:

класс информационных технологий, оснащенный рабочими местами на базе вычислительной техники с установленной интегрированной средой разработки программного обеспечения на языке C/C++ (Microsoft Visual C++ Express Edition, Microsoft Visual Studio, CodeBlocks или аналогичные).

**Б.1.О.18. Дисциплина «Методы программирования»**

Коды формируемых компетенций: ОПК-7.

В результате изучения дисциплины студент должен

знать:

- основные структуры данных, основные комбинаторные и теоретико-графовые алгоритмы;

- методику оценки вычислительной сложности алгоритма;

- способы эффективной реализации алгоритмов;

уметь:

- проводить оценку вычислительной сложности алгоритма;

владеть:

- навыками выбора и разработки алгоритмов при решении типовых задач программирования.

Примерное распределение часов: трудоемкость дисциплины 4 з.е., 144 час.

Форма контроля: экзамен.

Содержание дисциплины:

**Базовые структуры данных.** Понятие структуры данных. Базовые структуры данных: множество, стек, очередь, дек, список, деревья, двоичные деревья поиска. **Алгоритмы.** Понятие алгоритма. Свойства и виды алгоритмов. Способы представления алгоритма. Основные характеристики алгоритмов. Оценка вычислительной сложности алгоритма. Возможности усовершенствования алгоритма. **Алгоритмы сортировки.** Основные понятия и классификация алгоритмов сортировки. Алгоритмы внутренней сортировки: вставками, обменами, выбором, слиянием и распределяющей. Оценка вычислительной сложности алгоритмов внутренней сортировки и способы их эффективной реализации. **Алгоритмы поиска.** Основные понятия и классификация алгоритмов поиска. Алгоритмы поиска в последовательно организованных структурах. Поиск в древовидных структурах. Хеширование и разрешение коллизий. **Алгоритмы генерации комбинаторных объектов.** Основные понятия. Алгоритмы порождения перестановок. Алгоритмы порождения подмножеств. Коды Грея. **Алгоритмы на графах.** Основные понятия. Способы задания графов. Остовные деревья минимальной стоимости и алгоритмы их построения. Алгоритмы нахождения кратчайших расстояний между вершинами.

Рекомендуемый перечень основной литературы:

1. Анашкина Н.В., Петухова Н.Н., Смольянинов В.Ю. Технологии и методы программирования. – М.: Издательский центр «Академия», 2012. – 384 с.

2. Ахо А.В., Хопкрофт Дж., Ульман Дж. Структуры данных и алгоритмы. –М.: Вильямс, 2016. – 400 с.

3. Кормен Т., Лейзерсон Ч., Ривест Р., Штайн К. Алгоритмы: построение   
и анализ. – М.: Издательский дом «Вильямс», 2016. – 1323 с.

4. Кнут Д.Э. Искусство программирования, том 3. Сортировка и поиск. – М.: Вильямс, 2014. - 822 с.

5. Седжвик Р. Алгоритмы на С++. – М.: Издательский дом «Вильямс», 2016. – 1056 с.

Перечень материально-технического обеспечения:

класс информационных технологий, оснащенный рабочими местами на базе вычислительной техники с установленной интегрированной средой разработки программного обеспечения на языке C/C++ (Microsoft Visual C++ Express Edition, Microsoft Visual Studio, CodeBlocks или аналогичные).

**Б.1.О.19. Дисциплина «Прикладные информационные технологии»**

Коды формируемых компетенций: ОПК-2.

В результате изучения дисциплины студент должен

знать:

- классификацию компьютерных систем, виды информационного взаимодействия и обслуживания, основы построения информационно-вычислительных систем;

- назначение, функции и обобщённую структуру операционных систем и типовые операционные системы, в том числе отечественного производства;

- типовые прикладные информационные технологии и программное обеспечение, используемое для решения задач профессиональной деятельности, в том числе системы баз данных, технологии распределенного реестра и искусственного интеллекта;

уметь:

- применять выбранные информационные технологии, программные средства системного и прикладного назначений для решения задач профессиональной деятельности.

Примерное распределение часов: трудоемкость дисциплины 5 з.е., 180 час.

Форма контроля: экзамен.

Содержание дисциплины:

**Архитектура и организация информационно-вычислительных систем.** Классификация и типовые архитектуры компьютерных систем. Принципы построения информационно-вычислительных систем. Виды информационного взаимодействия и обслуживания. Клиент-серверное взаимодействие. Понятие «информационная технология» и её составляющие. Системное и прикладное программное обеспечение. **Операционные системы.** Понятие операционной системы. Функции и классификация операционных систем (ОС). Структура обобщённой ОС. Архитектура ОС Windows и ОС Linux, их основные компоненты. Файловые системы. Виртуализация. ОС отечественного производства. **Системы управления базами данных (СУБД).** Основы организации хранения данных   
в СУБД. Типы баз данных. Типы данных. Отношения между данными внутри БД. Нормализация. Язык запросов SQL. Выборка данных из нескольких таблиц. Объединяющие запросы. Создание индексов. Создание резервной копии данных   
и восстановление. Доступ к СУБД из различных приложений с использованием выбранного языка программирования. **Прикладное программное обеспечение.**

Рекомендуемый перечень лабораторных работ:

1. Установка и настройка выбранной операционной системы.

2. Получение данных из базы данных: составление SQL запросов.

3. Взаимодействие программ с СУБД.

Рекомендуемый перечень основной литературы:

1. Таненбаум Э. Современные операционные системы. 4-е изд. – СПб.: Питер, 2015. – 1120 с.: ил.

2. Васвани В. MySQL: использование и администрирование; пер. с англ. – СПб.: Питер, 2011. – 368 с.: ил.

3. Грошев А.С., Закляков П.В. Информатика: учеб. для вузов – 3-е изд., перераб. и доп. – М.: ДМК Пресс, 2016. – 588 с.: цв. ил.

Перечень материально-технического обеспечения:

класс информационных технологий, оснащенный рабочими местами на базе вычислительной техники с установленным программным обеспечением:

- операционные системы семейства Linux актуальной версии (CentOS, AltLinux, Debian, Ubuntu, AstraLinux, СинтезОС, GosLinux и другие);

- СУБД MySQL;

- средства виртуализации Oracle VM Virtual Box или аналогичные.

**Б.1.О.20. Дисциплина «Сети и системы передачи информации»**

Коды формируемых компетенций: ОПК-13, ОПК-14.

В результате изучения дисциплины студент должен

знать:

- эталонную модель взаимодействия открытых систем, основные протоколы и стандарты, используемые в сетях и системах электрической связи;

- основные системы и сети электрической связи, включая локальные и глобальные сети, сеть «интернета вещей», принципы их построения и технические характеристики входящих в них элементов;

- состав и основные характеристики технических средств сетей электросвязи;

уметь:

- оценивать технические возможности основных систем и сетей электрической связи;

- эксплуатировать и настраивать типовые технические средства сетей электросвязи, проводить диагностику типовых неисправностей в работе средств связи сетей электросвязи и исправлять их.

Примерное распределение часов: трудоемкость дисциплины 8 з.е., 288 час.

Форма контроля: 2 экзамена, курсовая работа.

Содержание дисциплины:

**Основы организации связи.** Принципы построения сетей связи: основные термины и определения, архитектура единой сети электросвязи, обобщенная структура телекоммуникационной сети, методы коммутации информации. Международные организации стандартизации в телекоммуникациях, Международный союз электросвязи (ITU). Эталонная модель взаимодействия открытых систем (OSI). **Телефонные сети и сети подвижной связи.** Телефонные сети общего пользования: архитектура и структура, качество предоставляемых услуг, сетевые технологии, сигнализация. Сети подвижной связи: основные стандарты, качество предоставляемых услуг, сетевые технологии, сигнализация. **Сети передачи данных.** Устройства объединения и защиты сетей. Технология Ethernet. Технологии виртуальных локальных сетей (VLAN). Технологии доступа с виртуальными каналами: технологии Х.25, Frame Relay, ATM. Технологии беспроводного доступа. Технологии транспортных телекоммуникационных сетей. Качество предоставляемых услуг. Сети на базе стека протоколов TCP/IP. Протоколы межсетевого уровня стека TCP/IP. Схема адресации протокола IP. Основы IP-маршрутизации. Система Domain Name System. Технология STP. Протоколы транспортного уровня TCP и UDP. Коммутация пакетов по меткам (MPLS). Качество предоставляемых услуг. **Принципы построения систем передачи информации.** Системы передачи информации (СПИ): структурные схемы систем передачи непрерывных и дискретных сообщений, функциональные элементы, основные характеристики. Сигналы электросвязи: классификация, временное и спектральное представление, основные характеристики сигналов. Первичные сигналы электросвязи: телефонные (речевые), факсимильные сигналы, сигналы радиовещания, телеграфные сигналы и сигналы передачи данных. Модели формирования и преобразования сигналов в аналоговых и цифровых СПИ. Анализ показателей помехоустойчивости и эффективности аналоговых и цифровых СПИ. Анализ показателей помехоустойчивости приема широкополосных сигналов.

**Многоканальные системы передачи.** Аналоговые многоканальные системы передачи (МСП): формирование группового сигнала, структурная схема и основные характеристики. Цифровые системы передачи (ЦСП) плезиохронной иерархии (PDH): основной цифровой канал, формирование цифровых потоков, структурная схема аппаратуры передачи и основные характеристики. Цифровые системы передачи синхронной иерархии (SDH): синхронный транспортный модуль (STM-1), формирование цифровых потоков, структурная схема аппаратуры передачи и основные характеристики. Волоконно-оптические системы передачи с многоволновым уплотнением каналов (WDM, DWDM): формирование оптических сигналов, структурная схема аппаратуры передачи и основные характеристики. Линейные тракты МСП: структура и состав аппаратуры передачи, принципы построения и основные характеристики. Анализ основных характеристик, оценка технических возможностей и показателей эффективности типовых многоканальных систем передачи информации.

**Системы радиосвязи.** Линии радиосвязи (радиолинии): структура радиолиний, виды радиоволн, используемые диапазоны радиоволн (радиочастот). Структура средств радиосвязи: антенно-фидерные, радиопередающие и радиоприемные устройства. Системы КВ радиосвязи: назначение, состав, принципы построения и основные характеристики. Системы радиорелейной связи: назначение, состав, принципы построения и основные характеристики. Системы тропосферной радиосвязи: назначение, состав, принципы построения и основные характеристики. Системы спутниковой связи: назначение, состав, типы орбит, принципы построения и основные характеристики. Системы сотовой подвижной радиосвязи: назначение, состав, принципы построения, технологии и основные характеристики. Системы транкинговой подвижной радиосвязи: назначение, состав, принципы построения, технологии и основные характеристики. Системы радиосвязи беспроводной телефонии: назначение, состав, принципы построения, технологии и основные характеристики. Тенденции и перспективы развития систем радиосвязи. Анализ основных характеристик, оценка технических возможностей и показателей эффективности систем радиосвязи.

Рекомендуемый перечень лабораторных работ:

1. Исследование коммутируемой локальной сети.

2. Исследование простой маршрутизируемой сети.

3. Настройка типовых технических средств сетей электросвязи.

4. Исследование помехоустойчивости и эффективности систем передачи информации.

Рекомендуемый перечень основной литературы:

1. Самуйлов К.Е., Шалимов И.А., Кулябов Д.С. Сети и системы передачи информации. Телекоммуникационные сети. Учебник и практикум – М.: Юрайт, 2016. – 364 с.

2. Мельников Д.А. Системы и сети передачи данных: Учебник. – М.: РадиоСофт, 2015. – 624 с.

3. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. – СПб.: Питер, 2016. – 992 с.

Перечень материально-технического обеспечения:

лаборатория сетей и систем передачи информации, оснащенная рабочими местами на базе вычислительной техники, стендами сетей передачи информации   
с коммутацией пакетов и коммутацией каналов, структурированной кабельной системой, телекоммуникационным оборудованием, эмулятором активного сетевого оборудования, специализированным программным обеспечением для настройки телекоммуникационного оборудования, анализа и генерации сигналов.

**Б.1.О.21. Дисциплина «Аппаратные средства телекоммуникационных систем»**

Коды формируемых компетенций: ОПК-14.

В результате изучения дисциплины студент должен

знать:

- элементную базу телекоммуникационных систем, включая области применения и основные характеристики, принципы организации систем на кристалле;

- основные архитектуры аппаратных средств телекоммуникационных систем и их отличия;

- технологии аппаратной обработки «больших данных», построения распределённых систем и систем искусственного интеллекта;

уметь:

- выбирать технологии и аппаратные средства телекоммуникационных систем и реализовывать на их основе отдельные узлы и устройства.

Примерное распределение часов: трудоемкость дисциплины 5 з.е., 180 час.

Форма контроля: экзамен.

Содержание дисциплины:

**Общие сведения об аппаратных средствах телекоммуникационных систем.** Современная технологическая база построения телекоммуникационных систем (ТКС). Поколения аппаратных средств ТКС. Универсальные и специализированные процессоры, программируемые логические интегральные схемы и массивно-параллельные процессоры как эффективные инструменты обработки сигналов и сообщений в ТКС. Системы на кристалле. **Специализированные процессоры.** Цифровые сигнальные процессоры**.** Классификация, характеристики и архитектуры цифровых сигнальных процессоров (ЦСП). Архитектура фон Неймана, гарвардская архитектура, особенности построения современных сигнальных процессоров. Поколения сигнальных процессоров. Сравнительная производительность ЦСП. Особенности построения вычислительных кластеров на базе ЦСП. Типовая система цифровой обработки сигналов на основе ЦСП. Архитектура и основные узлы типовых ЦСП. Разработка программного обеспечения для ЦСП**.** Стандартные и специализированные библиотеки функций реального времени для ЦСП. Особенности реализации функций на языках высокого уровня и ассемблера для ЦСП, оценка производительности. **Программируемые логические интегральные схемы (ПЛИС).** Элементная база ПЛИС. Системы автоматизации проектирования (САПР) устройств на ПЛИС. Общие сведения и характеристики современных САПР. Языки описания аппаратуры. Реализация алгоритмов цифровой обработки сигналов на ПЛИС. Проектирование систем на кристалле. **Массивно-параллельные процессоры (МПП).** Особенности архитектуры МПП, поколения МПП. Области применения МПП. Программно-аппаратная платформа для вычислений на GPU. Вычислительное ядро МПП, иерархическая структура ядра. МПП как параллельный потоковый процессор. Типы параллелизма. Многоуровневая модель памяти. Разработка программного обеспечения для массивно-параллельных процессоров. Технологии произвольных вычислений на МПП. Использование МПП в параллельных математических расчетах, системах обработки «больших данных» и системах искусственного интеллекта, составление алгоритмов цифровой обработки сигналов.

Рекомендуемый перечень лабораторных работ:

1. Реализация параллельных вычислений на ЦСП.

2. Моделирование учебной схемы для ПЛИС в симуляторе.

3. Программирование ядра МПП, создание вычислительной процедуры МПП.

4. Использование сторонних алгебраических библиотек.

Рекомендуемый перечень основной литературы:

1. Новожилов О.П. Основы микропроцессорной техники: Учебное пособие в 2-х томах. – М.: ИП Радиософт, 2007.

2. Стешенко В.Б. ПЛИС фирмы «Altera»: элементная база, система проектирования и языки описания аппаратуры. – М.: Додема XXI, 2002. – 573 с.

3. Кузелин М.О., Кнышев Д.А., Зотов В.Ю. Современное семейство ПЛИС фирмы Xilinx. – М.: Горячая линия–Телеком, 2004. – 440 с.

Перечень материально-технического обеспечения:

лаборатория (класс) цифровой обработки сигналов, оснащенный рабочими местами на базе вычислительной техники с поддержкой вычислений общего назначения на графических процессорах, платами цифровой обработки сигналов на базе сигнальных процессоров и программируемых логических интегральных схем, средствами разработки приложений для них.

**Б.1.О.22. Дисциплина «Измерения в телекоммуникационных системах»**

Коды формируемых компетенций: ОПК-12, ОПК-15.

В результате изучения дисциплины студент должен

знать:

- принципы построения и работы измерительных устройств и приборов;

- методики обработки и оценки достоверности результатов измерений;

- методики измерения и оценки параметров в телекоммуникационных системах и сетях;

уметь:

- проводить измерения в спектральной и временной областях;

- анализировать пропускную способность и предельную нагрузку сети связи, параметры передачи кадров при прохождении по каналам связи, проверять достижимость абонентов сети связи.

Примерное распределение часов: трудоемкость дисциплины 4 з.е., 144 час.

Форма контроля: экзамен.

Содержание дисциплины:

**Современное состояние измерений в телекоммуникационных системах.** Классификация измерительной аппаратуры. Классические средства измерений. Измерительные технологии современных телекоммуникаций. Метрологическое обеспечение телекоммуникационных систем. **Радиочастотные измерения.** Исследования формы и параметров сигнала. Измерения параметров спектра сигналов. Измерения мощности. Измерения напряженности электромагнитных полей. Измерительные генераторы. Измерение шумов и помех. **Измерения в цифровых системах передачи.** Измерения параметров физического уровня Е1. Оценка влияния битовых ошибок на параметры цифровых систем передачи в синхронных и асинхронных каналах, их нормирование и измерение (ES и SES). Измерение фазового дрожания. Измерения в каналах в PDN/SDN и ATM системах передачи. **Измерения на волоконно-оптических линиях связи.** Измерение потерь на волоконно-оптической линии. Измерение коэффициента затухания на оптической линии. Методы определения неоднородностей на оптической линии. Измерение дисперсии волокна. **Сетевые измерения.** Группы измерений, характерные для вторичных сетей связи. Измерения характеристик потоков данных на сетевом уровне. Анализаторы протоколов.

Рекомендуемый перечень лабораторных работ:

1. Измерения формы и параметров сигналов на физическом уровне.

2. Измерения характеристик потоков данных на сетевом уровне.

Рекомендуемый перечень основной литературы:

1. Хамадулин Э.Ф. Методы и средства измерений в телекоммуникационных системах: Учеб. пособие для академического бакалавриата – М.: «Юрайт», 2016. – 365 с.

Перечень материально-технического обеспечения:

лаборатория измерений в телекоммуникационных системах, оснащенная рабочими местами на базе вычислительной техники, структурированной кабельной системой, стендами для исследования параметров сетевого трафика, элементами телекоммуникационных систем с различными типами линий связи (проводных, беспроводных), комплектом измерительного оборудования для исследования параметров телекоммуникационных систем.

**Б.1.О.23. Дисциплина «Моделирование систем и сетей телекоммуникаций»**

Коды формируемых компетенций: ОПК-12.

В результате изучения дисциплины студент должен

знать:

- принципы и основные этапы математического и имитационного моделирования, походы к формализации явлений и процессов телекоммуникационных систем, типовые модели объектов, явлений и процессов телекоммуникационных систем;

- основные возможности избранного средства моделирования объектов, явлений и процессов телекоммуникационных систем;

уметь:

- разрабатывать модели и проводить математическое и имитационное моделирование типовых объектов, явлений и процессов телекоммуникационных систем.

Примерное распределение часов: трудоемкость дисциплины 5 з.е., 180 час.

Форма контроля: экзамен, курсовая работа.

Содержание дисциплины:

**Общие принципы моделирования систем и сетей телекоммуникаций.** Принципы формализации процессов функционирования систем и сетей телекоммуникаций. Принципы и основные этапы математического и имитационного моделирования систем и сетей телекоммуникаций. Понятия «модель системы телекоммуникаций», «модель сети телекоммуникаций». Принципы построения моделей системы и сети телекоммуникаций. **Средства моделирования систем и сетей телекоммуникаций.** Обзор средств моделирования систем и сетей телекоммуникаций. **Типовые модели систем и сетей телекоммуникаций.** Моделирование типовых устройств, систем и сетей телекоммуникаций.

Рекомендуемый перечень лабораторных работ:

1. Исследование типовых устройств, систем и сетей телекоммуникаций   
и показателей их эффективности.

Рекомендуемый перечень основной литературы:

1. Степанов С.Н. Теория телетрафика: концепции, модели, приложения. – М.: Горячая линия-Телеком, 2015. – 868 с.

Перечень материально-технического обеспечения:

компьютерный класс, оснащенный рабочими местами на базе вычислительной техники с установленным программным обеспечением, предназначенным для математических вычислений и моделирования (MATLAB R2014 и выше или аналогичное).

**Б.1.О.24. Дисциплина «Основы информационной безопасности»**

Коды формируемых компетенций: ОПК-1.

В результате изучения дисциплины студент должен

знать:

- место и роль информационной безопасности в системе национальной безопасности Российской Федерации;

- сущность и понятие информационной безопасности, характеристику ее составляющих.

Примерное распределение часов: трудоемкость дисциплины 3 з.е., 108 час.

Форма контроля: зачет.

Содержание дисциплины:

**Информационная безопасность государства.** Информационная безопасность Российской Федерации. Угрозы информационной безопасности Российской Федерации. Доктрина информационной безопасности. Общие принципы защиты информации. **Информационная война. Средства защиты и нападения.** Информационная война и информационное оружие. Особенности технических средств информационной войны. Классификация средств защиты и нападения. Классификация электронных устройств перехвата информации, внедряемых в средства вычислительной техники. Средства СДВ (Силовое Деструктивное Воздействие). **Уничтожение информации.** Необходимость уничтожения документов. Особенности удаления информации с электронных носителей. Политика уничтожения данных. Уничтожение конфиденциальной информации (плановое и экстренное). Следы в сети. Уникальные идентификаторы интернет-пользователей и электронные «отпечатки». Конфиденциальность в социальных сетях.

Рекомендуемый перечень основной литературы:

1. Нестеров С.А. Основы информационной безопасности. Учебное пособие. – М.: Лань, 2016. – 324 с.

**Б.1.О.25. Дисциплина «Организационное и правовое обеспечение информационной безопасности»**

Коды формируемых компетенций: ОПК-5, ОПК-6.

В результате изучения дисциплины студент должен

знать:

- нормативную правовую основу организации лицензирования отдельных видов деятельности в области защиты информации, сертификации средств защиты информации и аттестации объектов информатизации;

- правовые основы организации защиты информации;

- правовую характеристику преступлений в сфере компьютерной информации и меры юридической ответственности за правонарушения и преступления в области защиты информации;

- назначение, структуру и состав системы обеспечения информационной безопасности Российской Федерации;

- организацию деятельности по обеспечению безопасности критически важной информационной инфраструктуры Российской Федерации, основные требования, предъявляемые к организации защиты информации ограниченного доступа в процессе функционирования сетей электросвязи;

- нормативные, руководящие и методические документы уполномоченных федеральных органов государственной власти по защите информации ограниченного доступа;

- задачи органов защиты государственной тайны и служб защиты информации на предприятиях;

- систему организационных мер, направленных на защиту информации ограниченного доступа;

уметь:

- применять юридические понятия и термины, нормативные правовые акты и нормативные методические документы в области защиты информации.

Примерное распределение часов: трудоемкость дисциплины 5 з.е., 180 час.

Форма контроля: зачет, экзамен.

Содержание дисциплины:

**Законодательство Российской Федерации в области информационной безопасности.** Компетенция органов государственной власти по обеспечению информационной безопасности. Система нормативных правовых актов, регулирующих обеспечение информационной безопасности в Российской Федерации. Концептуальные документы в сфере информационной безопасности. Федеральные законы. Основные подзаконные акты. Нормативная база ФСТЭК России в сфере информационной безопасности. Правонарушения и преступления в сфере информационных технологий. Преступления в сфере компьютерной информации: виды, состав. Основы расследования преступлений в сфере компьютерной информации. Иные преступления в информационной сфере. Развитие зарубежных стандартов в сфере информационной безопасности. Система государственных и отраслевых стандартов в сфере информационной безопасности. **Правовой режим защиты государственной тайны.** Понятие правового режима защиты государственной тайны. Система нормативных правовых актов, регламентирующих обеспечение сохранности сведений, составляющих государственную тайну в Российской Федерации. Государственная тайна как особый вид защищаемой информации и ее характерные признаки. Принципы и механизмы отнесения сведений к государственной тайне, их засекречивания и рассекречивания. Органы защиты государственной тайны и их компетенция. Система контроля за состоянием защиты государственной тайны. Организационные меры, направленные на защиту государственной тайны. Режим секретности как основной порядок деятельности в сфере защиты государственной тайны. Юридическая ответственность за нарушения правового режима защиты государственной тайны (уголовная, административная, дисциплинарная). **Правовые режимы защиты информации конфиденциального характера.** Понятие информации конфиденциального характера по российскому законодательству. Основные виды информации конфиденциального характера: персональные данные, служебная тайна, коммерческая тайна, банковская тайна, профессиональная тайна, тайна следствия и судопроизводства. Правовые режимы информации конфиденциального характера: содержание и особенности. Основные требования, предъявляемые к организации защиты информации конфиденциального характера. Юридическая ответственность за нарушения правовых режимов «конфиденциальной» информации (дисциплинарная, гражданско-правовая, административная и уголовная). **Государственное регулирование деятельности в области защиты информации.** Понятие лицензирования по российскому законодательству. Виды деятельности, подлежащие лицензированию. Правовая регламентация лицензионной деятельности в области обеспечения информационной безопасности. Объекты лицензирования и участники лицензионных отношений в сфере защиты информации. Органы лицензирования и их полномочия. Организация лицензирования в сфере обеспечения информационной безопасности. Контроль за соблюдением лицензиатами условий ведения деятельности. Понятие подтверждения соответствия по российскому законодательству, формы подтверждения. Правовая регламентация сертификационной деятельности в области обеспечения информационной безопасности. Режимы сертификации. Объекты сертификационной деятельности (сертификации). Органы сертификации и их полномочия. **Правовое регулирование защиты информации в области связи.** Законодательство Российской Федерации в области связи. Государственное регулирование деятельности в области связи и защиты информации в области связи.

Рекомендуемый перечень основной литературы:

1. Полякова Т.А., Стрельцов А.А., Чубукова С.Г., Ниесов В.А. Организационное и правовое обеспечение информационной безопасности. Учебник и практикум для бакалавриата и магистратуры. / Под ред. Т.А. Поляковой, А.А. Стрельцова – М.: Юрайт, 2016. – 325 с.

2. Жигулин Г.П. Организационное и правовое обеспечение информационной безопасности. Учебное пособие. – СПб: НИУ ИТМО, 2014. – 173 с.

**Б.1.О.26. Дисциплина «Защита информации от утечки по техническим каналам»**

Коды формируемых компетенций: ОПК-9.

В результате изучения дисциплины студент должен

знать:

- технические каналы утечки информации;

- методы, способы и средства защиты информации от утечки по типовым техническим каналам на объектах информатизации;

уметь:

- проводить предпроектное обследование объекта информатизации с целью выявления потенциальных технических каналов утечки информации;

- обосновывать рациональный состав средств защиты информации от утечки по техническим каналам для защиты объекта информатизации;

- устанавливать и настраивать средства защиты информации от утечки по техническим каналам.

Примерное распределение часов: трудоемкость дисциплины 5 з.е., 180 час.

Форма контроля: экзамен.

Содержание дисциплины:

**Нормативно-правовые документы в области технической защиты информации (ТЗИ).** Концепция, организация и методология технической защиты информации. Нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа, проектирования средств защиты информации, сертификации средств защиты информации на соответствие требованиям по безопасности информации и аттестации объектов информатизации на соответствие требованиям по защите информации. Основные понятия и определения. Цели и задачи ТЗИ. **Определение технического канала утечки информации.** Структурная схема технического канала утечки информации. Классификация и характеристики технических каналов утечки информации. **Физическая защита объектов информатизации.** Общие положения концепции защиты объектов. Назначение, виды и основные характеристики систем охраны, используемых на объектах информатизации. **Методы и средства ТЗИ.** Содержание работ, организационно-распорядительные документы, аттестация, сертификация. Средства защиты. Организационные и технические средства и системы защиты. Взаимодействие средств защиты. Основные и вспомогательные средства защиты. Принципы построения средств защиты. Техническая защита помещений и технических средств обработки информации. Методы и технологии защиты информации от несанкционированного доступа и специальных программных воздействий на нее. Типовые нарушения в организации и осуществлении ТЗИ. **Методы и средства контроля эффективности ТЗИ.** Показатели эффективности защиты информации, обрабатываемой техническими средствами. Методы контроля защищенности информации от несанкционированного доступа и специальных программных воздействий на нее. Методы контроля эффективности защиты информации от утечки по техническим каналам. Средства контроля эффективности защиты информации от утечки по техническим каналам. Методы и методики проведения измерений, оценки и обработки их результатов.

Рекомендуемый перечень лабораторных работ:

1. Побочные электромагнитные излучения средств вычислительной техники.

2. Электромагнитные наводки от средств вычислительной техники в линейных коммуникациях.

3. Защита от побочных электромагнитных излучений средств вычислительной техники пространственным зашумлением.

4. Пассивные и активные методы защиты от наводки средств вычислительной техники в линейных коммуникациях.

Рекомендуемый перечень основной литературы:

1. Бузов Г.А. Защита информации ограниченного доступа от утечки по техническим каналам, справочное издание, 2017.

2. Технические средства и методы защиты информации: учебник. / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков. – 7-е изд., испр. и доп. – М.: Горячая линия-Телеком, 2018. – 444 с.

3. Меньшаков Ю.К. Основы защиты от технических разведок: учебное пособие, 2011.

Перечень материально-технического обеспечения:

лаборатория технической защиты информации, оснащенная специализированным оборудованием по защите информации от утечки по акустическому, акустоэлектрическому каналам, каналу побочных электромагнитных излучений и наводок, техническими средствами контроля эффективности защиты информации от утечки по указанным каналам.

**Б.1.О.27. Дисциплина «Методы и средства криптографической защиты информации»**

Коды формируемых компетенций: ОПК-10.

В результате изучения дисциплины студент должен

знать:

- основные понятия криптографии и криптографические методы защиты информации;

- основные типы средств криптографической защиты информации и предъявляемые к ним требования;

- основные криптографические алгоритмы и механизмы, определяемые национальными стандартами и рекомендациями Российской Федерации, и стандартами международной организации по стандартизации;

уметь:

- осуществлять обоснованный выбор и использовать средства криптографической защиты информации при решении задач профессиональной деятельности.

Примерное распределение часов: трудоемкость дисциплины 5 з.е., 180 час.

Форма контроля: экзамен.

Содержание дисциплины:

**Введение в криптографию.** Открытые сообщения и их характеристики. История криптографии. Примеры ручных шифров. Основные этапы становления криптографии как науки. Частотные характеристики открытых текстов. *k*-граммная модель открытого текста. Критерии распознавания открытого текста. Основные задачи и понятия криптографии. Перечень угроз. Симметричное и асимметричное шифрование в задачах защиты информации. Шифры с открытым ключом и их использование. Классификация шифров. Модели шифров. Основные требования к шифрам. Простейшие криптографические протоколы. **Основные классы шифров и их свойства.** Шифры перестановки. Разновидности шифров перестановки: маршрутные и геометрические перестановки. Элементы криптоанализа шифров перестановки. Поточные шифры замены. Шифры простой замены и их анализ. Многоалфавитные шифры замены. Шифры гаммирования и их анализ. Использование неравновероятной гаммы, повторное использование гаммы, криптоанализ шифра Виженера. Тесты У. Фридмана. Блочные шифры простой замены и особенности их анализа. Современные блочные шифры. Криптоалгоритмы ГОСТ-28147-89 и «Магма». КриптоалгоритмыAES, «Кузнечик». **Надёжность шифров.** Основы теории К. Шеннона. Криптографическая стойкость шифров. Теоретически стойкие шифры. Шифры, совершенные при нападении на открытый текст. Шифры, совершенные при нападении на ключ. О теоретико-информационном подходе в криптографии. Энтропия и количество информации. «Ненадёжность шифра», «ложные ключи» и «расстояние единственности». Практически стойкие шифры. Вопросы имитозащиты. Имитостойкость шифров. Характеристики имитостойкости шифров и их оценки. Примеры имитостойких и неимитостойких шифров. Методы имитозащиты неимитостойких шифров. Имитовставки. Коды аутентификации. Помехоустойчивость шифров. Понятие о помехоустойчивости шифра. Шифры, не размножающие искажений типа замены знаков. Шифры, не размножающие искажений типа пропуск-вставка знаков. **Методы синтеза и анализа криптографических алгоритмов с секретным ключом.** Принципы построения криптографических алгоритмов. Принципы построения алгоритмов блочного шифрования. Выбор базовых преобразований. Режимы использования блочных шифров и их особенности. Принципы построения алгоритмов поточного шифрования. Режимы использования поточных шифров. Строение поточных шифрсистем. Типовые генераторы псевдослучайных последовательностей. Конгруэнтные генераторы. Генераторы Фибоначчи. Генераторы, основанные на сложнорешаемых задачах теории чисел. Генераторы на основе линейных регистров сдвига. Линейные рекуррентные последовательности (ЛРП) над полем. Свойства ЛРП максимального периода. Линейная сложность псевдослучайной последовательности. Методы усложнения ЛРП. Фильтрующие и комбинирующие генераторы, и их свойства. Композиции линейных регистров сдвига. Методы анализа криптографических алгоритмов. Подходы к анализу криптографических алгоритмов. Метод перебора. Корреляционный метод анализа поточных шифров. Линейный и дифференциальный методы анализа блочных шифров. **Методы синтеза и анализа криптографических алгоритмов с открытым ключом.** Системы шифрования с открытым ключом. Шифрсистема RSA. Шифрсистема Эль-Гамаля. Шифрсистема на основе задачи об «укладке рюкзака». Анализ шифрсистемы RSA. Практические аспекты использования шифрсистем с открытым ключом. Алгоритмы цифровых подписей. Цифровые подписи на основе шифрсистем с открытым ключом. Цифровая подпись Фиата-Шамира. Цифровая подпись Эль-Гамаля. Стандарты цифровой подписи. Алгоритмы идентификации. Протоколы типа запрос-ответ. Протоколы, использующие цифровую подпись. Протоколы с нулевым разглашением. Алгоритмы распределения ключей. Алгоритмы передачи ключей (с использованием и без использования цифровой подписи). Алгоритмы открытого распределения ключей. Алгоритмы предварительного распределения ключей. **Хеш-функции и их криптографические приложения.** Общие сведения о хеш-функциях. Функция хэширования «Стрибог». Ключевые и бесключевые хеш-функции. Итеративные способы построения хеш-функций. Понятие о стойкости хеш-функции. Целостность данных и аутентификация источника данных. Конструкции систем аутентификации на основе хеш-функций. Коды аутентичности сообщений: HMAC, UMAC.Конструкции MAC на основе симметричного шифрования. Система CBC-MAC. Основы анализа CBC-MAC: атака на основе наличия коллизий, использование CBC-MAC для аутентификации сообщений переменной длины. Другие системы: EMAC, XOR-MAC, PCS-MAC. Системы, совмещающие конфиденциальность и аутентификацию на одном ключе: ССМ, ОСВ.

Рекомендуемый перечень основной литературы:

1. Лось А.Б., Нестеренко А.Ю., Рожков М.И. Криптографические методы защиты информации: учебник для академического бакалавриата. – М.: Издательство Юрайт, 2016. – 473 с.

2. Фомичёв В.М., Мельников Д.А. Криптографические методы защиты информации. В 2 ч. Часть 1. Математические аспекты: учебник для академического бакалавриата. – М.: Издательство Юрайт, 2017. – 209 с.

3. Фомичёв В.М., Мельников Д.А. Криптографические методы защиты информации. В 2 ч. Часть 2. Системные и прикладные аспекты: учебник для академического бакалавриата. – М.: Издательство Юрайт, 2017. – 245 с.

4. Васильева И.Н. Криптографические методы защиты информации: учебник и практикум для академического бакалавриата. – М.: Издательство Юрайт, 2017. –   
349 с.

Перечень материально-технического обеспечения:

компьютерный класс, оснащенный рабочими местами на базе вычислительной техники с установленным программным обеспечением:

- для математических вычислений (MATLAB, MAPLE или MATHEMATICA или аналогичное);

- отечественными средствами криптографической защиты информации, сертифицированными ФСБ России и доступными для свободного скачивания.

**Б.1.О.28. Дисциплина «Программно-аппаратные средства защиты информации телекоммуникационных систем»**

Коды формируемых компетенций: ОПК-9.

В результате изучения дисциплины студент должен

знать:

- основные программные и программно-аппаратные средства защиты информации телекоммуникационных систем от несанкционированного доступа и принципы работы этих средств;

уметь:

- настраивать типовые программные и программно-аппаратные средства защиты информации телекоммуникационных систем от несанкционированного доступа.

Примерное распределение часов: трудоемкость дисциплины 5 з.е., 180 час.

Форма контроля: экзамена.

Содержание дисциплины:

**Подсистемы защиты современных операционных систем.** Субъекты, объекты, методы и права доступа в современных операционных системах. Основные компоненты подсистем защиты UNIX и Windows. Управление доступом, аутентификация, аудит. Основные проблемы с безопасностью и возможные решения в современных операционных системах. **Защита информации в вычислительных сетях.** Атаки на сетевые службы, типы угроз, классификация атак по основным механизмам реализации угроз. Сетевые сканеры. Пакетные фильтры и межсетевые экраны, их классификация и особенности применения. Виртуальные частные сети. Управление доступом в телекоммуникационных системах. **Защита информации в системах управления базами данных.** Угрозы безопасности баз данных: общие и специфичные. Модели безопасности систем управления базами данных (СУБД). Средства и методы обеспечения целостность данных в СУБД. Ролевое разграничение доступа к данным в современных СУБД. **Антивирусная защита компьютерных систем.** Понятие компьютерного вируса, типичные предпосылки к внедрению компьютерных вирусов. Принципы построения политики безопасности, обеспечивающей высокую защищенность от вредоносного программного обеспечения: принцип минимизации программного обеспечения, принцип минимизации полномочий пользователей. Специализированные средства и методы выявления вредоносных программ: сигнатурное и эвристическое сканирование, контроль целостности, мониторинг информационных потоков, изолированная программная среда, программные ловушки.

Рекомендуемый перечень лабораторных работ:

1. Подсистема дискреционного доступа операционной системы Linux.

2. Подсистема аутентификации операционной системы Linux.

3. Подсистема дискреционного доступа операционной системы Windows.

4. Подсистема аутентификации операционной системы Windows.

5. Программы анализа сетевого трафика в ОС Windows и ОС Linux.

6. Межсетевой экран в ОС Linux.

7. Антивирусная защита операционной системы Windows.

Рекомендуемый перечень основной литературы:

1. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – М.: ДМК Пресс, 2012. – 592 с.

2. Чипига А.Ф. Информационная безопасность автоматизированных систем: учебное пособие для вузов. – М.: Гелиос АРВ, 2010 г. – 335 с.

Перечень материально-технического обеспечения:

лаборатория программно-аппаратных средств защиты информации, оснащенную антивирусными программными комплексами, аппаратными средствами аутентификации пользователя, программно-аппаратными комплексами защиты информации от несанкционированного доступа, включающими в том числе средства криптографической защиты информации.

**Б.1.О.29. Дисциплина «Проектирование защищенных телекоммуникационных систем»**

Коды формируемых компетенций: ОПК-8, ОПК-16.

В результате изучения дисциплины студент должен

знать:

- основные формы, методы и приемы научного исследования, применяемые при проведении разработок в области функционирования, развития и обеспечения информационной безопасности телекоммуникационных систем и сетей;

- общие принципы проектирования систем и сетей электрической связи и принципы построения защищенных телекоммуникационных систем;

- номенклатуру и содержание нормативных правовых актов и нормативных методических документов, применяемых при проектировании защищенных телекоммуникационные систем;

- состав технико-экономического обоснования проектируемых защищенных телекоммуникационных систем;

уметь:

- разрабатывать необходимую техническую документацию в области проектирования защищенных телекоммуникационные систем с учетом действующих нормативных и методических документов;

- проводить подготовку исходных данных для технико-экономического обоснования проектируемых защищенных телекоммуникационных систем.

Примерное распределение часов: трудоемкость дисциплины 5 з.е., 180 час.

Форма контроля: экзамен.

Содержание дисциплины:

**Методология проектирования защищенных телекоммуникационных систем.** Понятие процесса проектирования защищенных телекоммуникационных систем. Постановка задачи управления процессом проектирования защищенных телекоммуникационных систем. Нормативные документы, применяемые при проектировании защищенных телекоммуникационные систем. Жизненный цикл проектируемых систем связи. Модели жизненного цикла. Документация по проектированию защищенной телекоммуникационной системы. Состав технического задания. Порядок формирования программ и методик испытаний системы связи и отдельных ее элементов. Примеры методик измерения характеристик элементов современных систем связи.

**Принципы построения защищенных телекоммуникационных систем** (по видам систем связи и их назначению). Основные формы, методы и приемы научного исследования, применяемые при защищенных телекоммуникационных систем. Особенности проектирования и разработки отдельных типовых элементов защищенных телекоммуникационных систем. Защита информации и каналов связи в различных условиях.

Рекомендуемый перечень основной литературы:

1. Крук Б.И, Попантонопуло В.Н., Шувалов В.П. Телекоммуникационные системы и сети: Учебное пособие. В 3 томах. Том 1 – Современные технологии. Под ред. профессора Шувалова В.П. – М.: Горячая линия–Телеком, 2003. –647 с.: ил.

2. Олифер В., Олифер Н. Компьютерные сети: принципы, технологии, протоколы. – СПб: Издательство: Питер, 2016. – 991 с.

3. Таненбаум Э. Компьютерные сети. – СПб: Издательство: Питер, 2016. –   
955 с.

Перечень материально-технического обеспечения:

компьютерный класс, оснащенный рабочими местами на базе вычислительной техники с установленным программным обеспечением, предназначенным для моделирования компьютерных сетей.

**Б.1.О.30. Дисциплина «Комплексное обеспечение защиты информации телекоммуникационных систем»**

Коды формируемых компетенций: ОПК-6, ОПК-13, ОПК-15.

В результате изучения дисциплины студент должен

знать:

- порядок организации защиты информации ограниченного доступа в процессе функционирования сетей электросвязи;

- основные уязвимости элементов информационно-телекоммуникационной инфраструктуры и принципы обеспечения её информационной безопасности;

- основные угрозы безопасности информации и модели нарушителя, принципы формирования политики информационной безопасности телекоммуникационной системы

- типовые средства для инструментальной оценки уровня защищённости телекоммуникационных систем;

уметь:

- организовать защиту информации ограниченного доступа в процессе функционирования сетей электросвязи в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

- анализировать угрозы информационно-телекоммуникационной инфраструктуре и циркулирующей в ней информации, выбирать необходимые средства для обеспечения информационной безопасности;

- проводить анализ защищенности информации от несанкционированного доступа в телекоммуникационных системах и сетях.

Примерное распределение часов: трудоемкость дисциплины 5 з.е., 180 час.

Форма контроля: экзамен.

Содержание дисциплины:

**Обеспечение информационной безопасности телекоммуникационных систем.** Классификация информации, циркулирующей в телекоммуникационной системе предприятия. Модели безопасности телекоммуникационной системы. Организационная модель информационной безопасности телекоммуникационных систем. Основные уязвимости элементов информационно-телекоммуникационной инфраструктуры. Особенности комплексного обеспечения информационной безопасности телекоммуникационных систем различных организаций. Политика информационной безопасности телекоммуникационной системы, принципы ее формирования. Угрозы безопасности телекоммуникационной системы, модель нарушителя и модель угроз. Обеспечение требований к качеству обслуживания в телекоммуникационной системе. **Анализ защищенности телекоммуникационных систем.** Характеристики защищенности телекоммуникационной системы. Анализ защищенности телекоммуникационной системы на основе отдельных характеристик защищенности. Место, задачи и классификация систем инструментальной оценки защищенности телекоммуникационных систем. Сетевые сканеры и размещение агентов сетевых сканеров. Принципы работы сетевых сканеров. Этапы работы сетевых сканеров. Критерии выбора систем анализа защищенности телекоммуникационных систем. Тесты на проникновение в телекоммуникационную систему. Организация проведения тестов. Программные средства проведения тестов на проникновение. Оценка результатов проведения тестов. Исследование защищенности мультипротокольного оборудования.

Рекомендуемый перечень лабораторных работ:

1. Исследование уязвимости мультипротокольного оборудования к сетевым атакам на выделенные каналы управления мультипротокольного оборудования.

2. Исследование защищенности мультипротокольного оборудования.

Рекомендуемый перечень основной литературы:

1. Тумбинская М.В., Петровский М.В. Комплексное обеспечение информационной безопасности на предприятии: учебник. – М.: Издательство Лань, 2019. – 344 с.

2. Гатчин Ю.А., Климова Е.В. Введение в комплексную защиту объектов информатизации: учебное пособие. – СПб: НИТУ ИТМО, 2011. – 112 с.

Перечень материально-технического обеспечения:

- лаборатория сетей и систем передачи информации, оснащенная рабочими местами на базе вычислительной техники, телекоммуникационным оборудованием (маршрутизирующий коммутатор RSOS 6850, маршрутизаторы Cisco любых моделей либо аналогичные им) и эмулятором активного сетевого оборудования.

- программное обеспечение: Kali Linux, FiksIdent, Cisco Packet Tracer или аналогичное.

**Б.1.С.6.1. Дисциплина «Телекоммуникационные системы комплексов координатно-временного обеспечения»**

Коды формируемых компетенций: ОПК-6.1.

В результате изучения дисциплины студент должен

знать:

- принципы построения и функционирования космических комплексов координатно-временного обеспечения;

- основные методы и средства защиты комплексов координатно-временного обеспечения;

уметь:

- проектировать защищенные телекоммуникационные системы в условиях воздействия радиопомех со стороны злоумышленника, низкого отношения сигнал/шум и влияния эффекта Доплера.

Примерное распределение часов: трудоемкость дисциплины 4 з.е., 144 час.

Форма контроля: экзамен

Содержание дисциплины:

**Сигналы координатно-временного обеспечения и их свойства.** Спектр сигнала. Мощность сигнала. Меандровая последовательность. Тактовая частота. Модулирующий сигнал. Поднесущая. Несущая. BOC-сигналы. Отношение сигнал/шум. Эффект Доплера. **Координатно-временное обеспечение в глобальных навигационных спутниковых системах (ГНСС).** Псевдослучайная кодовая последовательность. Системное время ГНСС. Цифровое поле. Принципы разделения сигналов в ГНСС. Навигационное сообщение. Дальномерные коды. Сигналы открытого доступа. Сигналы закрытого доступа. Корреляционный интеграл. Разрешение сигналов. **Кодирование сигналов.** Огибающая кода. Свёрточный код. Оверлейный код. Кодер. Последовательность Касами. **Помехозащита и помехоустойчивость сигналов космических аппаратов (КА).** Генератор имитационных помех. Апостериорная плотность вероятности задержки сигнала. Фильтрация задержек дальномерного кода. Метод дополнительной переменной. Автокорреляционная функция. Шифратор. Помехозащищённость. Помехоустойчивость. Криптостойкость. Рекуррентный генератор последовательности чисел. Синхропосылка. Уравнение расшифрования. Уплотнение. Информационная и пилотная компоненты сигнала. Полосовые фильтры. Режекторные фильтры. «BPSK-type» методы. ECDS алгоритм. **Идеология SAASM.** Красный ключ. Кодирование конверта. Чёрный ключ. **Методы контроля подлинности навигационного сигнала.** SSSC-коды. NMA-метод. VSD-защита. Метод двойного приёмника. **Обеспечение имитостойкости сигналов КА.** Приёмник навигационных сигналов с санкционированным доступом. Антиимитационные последовательности. Антиимитационная модуляция. Ключи. Итерационный ключ. Развертывание ключа. Таблица замен. Узлы замен. Криптопреобразование. Кодирование. Зашифрование. Расшифрование. Случайные коды. Режим прямой замены по ГОСТ 28147-89. Режим простой замены. Режим гаммирования. Режим гаммирования с обратной связью. Режим выработки имитовставки. Конкатация данных.

Рекомендуемый перечень лабораторных работ:

1. Принципы координатно-временного обеспечения потребителей в ГНСС;

2. Методы обеспечения имитостойкости сигналов КА;

3. Методы контроля подлинности навигационного сигнала.

Рекомендуемый перечень основной литературы:

1. Поваляев А.А., Вейцель А.В., Мазепа Р.Б. «Глобальные спутниковые системы синхронизации и управления движением в околоземном пространстве». – М.: Вузовская книга, 2012.

2. Шатилов А.Ю. Характеристики радиосигналов глобальных спутниковых радионавигационных систем ГЛОНАСС, GPS, GALILEO, BEIDOU и функциональных дополнений SBAS: учебное пособие. – М.: МЭИ, 2015.

3. Майстренко В.А., Соловьёв А.А., Пляскин М.Ю., Тихонов А.И. Современные информационные каналы и системы связи. – Омск: ОГТУ, 2017.

4. Зверев В.А., Стромков А.А. Выделение сигналов из помех численными методами. – Нижний Новгород: ИПФ РАН, 2001. – 188 с.

5. Васильева И.Н. Криптографические методы защиты информации. – М.: Издательство Юрайт, 2020.

Перечень материально-технического обеспечения:

- приёмник сигналов ГНСС GPS/ГЛОНАСС (Javad / Topcon / Ashtech) с программным обеспечением NetView;

- навигационная антенна для работы в диапазонах L1/L2 Javad GrAnt или аналогичная;

- имитатор навигационных сигналов с частотным и кодовым разделением ИМ-2 с поставляемым с ним соответствующим программным обеспечением, Spirent GSS-серии с программным обеспечением SimGen;

- мультиплексор ГНСС сигналов на 2 входа (TNC/BNC/SMA/CRC9);

- компьютерный класс, оснащенный рабочими местами на базе вычислительной техники с установленным программным обеспечением, предназначенным имитации сигналов в среде MATLAB или аналогичный.

**Б.1.С.6.2. Дисциплина «Проектирование защищенных телекоммуникационных систем в контуре управления космическим аппаратом»**

Коды формируемых компетенций: ОПК-6.1.

В результате изучения дисциплины студент должен

знать:

- принципы построения и функционирования телеметрических систем;

- принципы построения и функционирования командных систем;

- основные принципы и классы управления космическими объектами;

уметь:

- проектировать защищенные телеметрические системы;

- проектировать защищенные командные системы.

Примерное распределение часов: трудоемкость дисциплины 5 з.е., 180 час.

Форма контроля: экзамен

Содержание дисциплины:

**Этапы функционирования космических аппаратов (КА).** Этап наземной эксплуатации. Этап выведения КА на целевую орбиту. Этап ввода в штатную эксплуатацию. Этап штатной эксплуатации. Вывод из целевого использования КА. Космическая система. Структура космической системы. Орбитальная группировка. Управление на различных фазах эксплуатации. **Задачи и способы управления КА.** Задачи управления КА: контроль движения КА на орбите, управление функционированием бортовых систем КА. Непосредственное и ретрансляционное управление. Измерение параметров движения КА. Обработка траекторной информации. Синхронизация бортового времени. Управление движением КА. Управление работой бортовой аппаратурой. Концепция автономности КА. Командное управление. Программно-временное управление. Управление с помощью полетных процедур. Телеметрический контроль КА. **Сигналы радиотехнических средств управления КА.** Основные требования, определяющие выбор сигнально-кодовых конструкций для систем телеметрии и телекоманд. Выбор сигнала для измерения дальности и радиальной скорости КА. Обеспечение требований по помехозащищенности радиолинии. Метод прямого последовательного расширения спектра. Метод расширения спектра скачкообразной перестройкой частоты. **Наземный технические средства управления.** Автоматизированная система управления КА. Командно-измерительные пункты. Структурная схема НКУ. Центр управления полетами. Информационно-вычислительный комплекс ЦУП. Баллистический центр и система единого времени. Структурно-функциональная схема наземной станции КИС. Типовая структурная схема передатчика КИС. Типовая структурная схема приемника КИС. Типовая структурно-функциональная схема системы наведения антенны. Основные характеристики КИС. Низкочастотная часть КИС. **Бортовые технические средства управления.** Бортовая аппаратура КИС. Задачи, функции, основные характеристики аппаратуры КИС. Режимы работы. Структурная схема. Назначение и характеристики составляющих элементов. Бортовой комплекс управления (БКУ). Задачи, функции, структура БКУ. Бортовой компьютер. Развитие и совершенствование БКУ. Бортовое программное обеспечение БКУ. **Телекомандная система.** Цель функционирования ТК-системы. Состав ТК системы. Телеуправление CCSDS. Уровни и сервисы уровней системы ТК. Структуры данных телекоманд. Уровень протокола передачи данных: управление потоком данных, сегментация, аутентификация, варианты формирования фреймов передачи, структура фрейма, расчет контрольной суммы. Уровень синхронизации и кодирования: рандомизация, БЧХ-кодирование, последовательность процедур при передаче и при приеме ТК. Телеуправление ESA: особенности, отличия от рекомендаций CCSDS. **Телеметрическая система.** Цель функционирования ТМ-системы. Состав ТМ системы. Телеметрия CCSDS. Иерархическая модель телеметрических служб. Структуры телеметрических данных. Содержание пакета источника. Сегментация. Сегмент пакета. Структура фрейма передачи. Уровень синхронизации и кодирования: последовательность процедур при передаче и при приеме ТК, сверточное кодирование, кодирование Рида-Соломона, турбокодирование, функции рандомизация, генератор псевдослучайной последовательности, структура псевдо-рандомизации. Телеметрия ESA: особенности, отличия от рекомендаций CCSDS. **Обеспечение аутентификации и конфиденциальности.** Общие подходы к процедуре аутентификации. Рекомендации CCSDS по обеспечению безопасности канала телеуправления. Протокол безопасности CCSDS. Структура телекоманды при аутентификации. Алгоритмы аутентификации. Способы реализации системы аутентификации. Рекомендуемые алгоритмы аутентификации. Требования к криптографическим алгоритмам. Рекомендации CCSDS по обеспечению конфиденциальности. Рекомендуемые алгоритмы шифрования. Способы реализация системы шифрования. Команды управления аутентификацией и криптографической системой. Аутентификация и шифрование при аварийных ситуациях. **Проектирования защищенных систем ТМ/ТК.** Фазы проектирования космической техники. Фаза проектирования системы ТМ/ТК. Разработка исходных требований к проектированию. Концептуальное проектирование: уточнение целевых параметров и системных компромиссов; уточнение аппаратного состава и их конструктивного исполнения; выработка технических требований в целом и к отдельным частям; оценка реализуемости. Предварительное (эскизное) проектирование: уточнения способа реализации; разработка основных технических решений; разработка схемотехники и программного обеспечения; макетирование устройства. Разработка технического проекта: уточнение и верификация ранее принятых технических решений; уточнение реализации принятых решений (схемотехника и программное обеспечение); изготовление опытного образца; подготовка плана функциональных испытаний. Функциональные испытания. Испытания на условия эксплуатации. Оценка результатов проектирование и принятия решения о достижимости исходных требований.

Рекомендуемый перечень лабораторных работ:

1. Моделирование сигналов в радиолиниях телеметрии/телекоманд в радиоизмерительном комплексе NI.

2. Наземная командно-измерительная система Cortex CRT-XL.

3. Бортовая аппаратура КИС в составе информационно-управляющего комплекса GR-RASTA.

4. Прием и декодирование телеметрической информации техническими средствами наземной станции.

Рекомендуемый перечень основной литературы:

1. Молотов Е.П. Наземные радиотехнические системы управления космическими аппаратами – М.: Физматлит, 2004. – 256 с.

2. Назаров В.А. и др. Современная телеметрия в теории и на практике: учебный курс. – СПб.: Наука и техника, 2007. – 672 с.

3. Кащеев Н.А. Радиотехнические средства управления космическими аппаратами [Электронный ресурс]: учебное пособие. – М., 2005. – 202 с.

4. Вейцель В.А. и др. Радиосистемы управления: учеб. для вузов. М.: Дрофа, 2005 – 416с.

5. Бортовые системы управления космическими аппаратами: Учебное пособие. / Бровкин А.Г., Бурдыгов Б.Г., Гордийко С.В. и др. Под редакцией А.С. Сырова. – М.: Изд-во МАИ-ПРИНТ, 2010.

Перечень материально-технического обеспечения:

радиотехнические комплексы GR RASTA, GR CORTEX, National Instruments (LabVIEW).

**Б.1.С.6.3. Дисциплина «Протоколы сетевого взаимодействия объектов аэрокосмического и наземного сегментов телекоммуникационной системы»**

Коды формируемых компетенций: ОПК-6.2.

В результате изучения дисциплины студент должен

знать:

- защищенные протоколы управления объектами аэрокосмического сегмента телекоммуникационной системы;

- сетевые протоколы информационного взаимодействия аэрокосмического и наземного сегментов и параметры их настройки;

- топологии и протоколы сетевого взаимодействия, применяемые в эксплуатируемых сетях наземного сегмента аэрокосмической телекоммуникационной системы;

уметь:

- устанавливать и настраивать параметры сетевых протоколов, реализованных в телекоммуникационном оборудовании объектов аэрокосмического и наземного сегментов;

- наблюдать и оценивать информационные потоки на объектах аэрокосмического и наземного сегментов с помощью пакетных анализаторов

владеть:

- основными приемами борьбы с уязвимостями реализаций протоколов сетевого взаимодействия, применяемых в эксплуатируемых сетях наземного сегмента аэрокосмической телекоммуникационной системы.

Примерное распределение часов: трудоемкость дисциплины 6 з.е., 216 час.

Форма контроля: экзамен

Содержание дисциплины:

**Основы сетевых технологий.** Роль сетей в информационной деятельности. Понятие о сетевых ресурсах. Разделение и распределение сетевых ресурсов. Архитектура локальных и распределенных сетей. Основные понятия и определения. Методы доступа к среде передачи данных в сетях. Характеристики среды передачи данных. Технология локальных сетей. Сетевое оборудование для формирования различных топологий. Выбор и оптимизация аппаратных средств. Глобальные сети. Структура и протоколы спутниковой системы мобильной и факсимильной связи. **Особенности соединений и адресации на физическом и логическом уровнях модели OSI.** Характеристика и параметры соединений на физическом уровне. Характеристика и параметры соединений на логическом уровне. Анализ критических параметров соединений и адресации. **Системный подход к проектированию защищенных протоколов.** Системный подход к безопасности информационного взаимодействия и его роль в разработке и применении безопасных протоколов и их настроек. Применение системного подхода для поиска уязвимостей в протоколах информационного взаимодействия. **Безопасность протоколов аэрокосмических телекоммуникационных систем.** Обеспечение безопасности открытых протоколов. Применение криптографических протоколов для защиты объектов аэрокосмического и наземного сегментов телекоммуникационных систем. Топология сети как средство защиты от атак. Использование специализированных средств анализа на примере WildPackets, CommView, Wireshark для целей активного выявления уязвимостей. Пример перехвата трафика при реализации атак. **Безопасность протоколов и их реализаций.** Основные характеристики и параметры протоколов, отражающих их защитные свойства. Проблемы безопасности популярных протоколов и их реализаций. Механизмы таймаутов и идентификации сессий, надежность доставки сообщений. Классификация методов и средств анализа безопасности протоколов. Сканирование сетевых служб как метод анализ безопасности реализации протокола. **Оптимизация протоколов информационного взаимодействия.** Принципы внутриуровневой и межуровневой оптимизации протоколов с целью повышения их защищенности. Системы обнаружения вторжений: виды и возможности в части оптимизации информационного взаимодействия. Параметрическая оптимизация протоколов: статические и динамические параметры. Доступ к сети, сторонние соединения и параметры протоколов.

Рекомендуемый перечень основной литературы:

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: учебное пособие. – 4-е изд. - М., СПб., Нижний Новгород: Питер, 2012. – 943 с.: ил.

2. Михайлов В.Ю., Мазепа Р.Б. Основы информационных технологий. Введение в процессы информационного взаимодействия: учебное пособие. – М.: Вузовская кн., 2012. – 60 с.

3. Карпухин Е.О. Технологии и методы защиты инфокоммуникационных систем и сетей: учебное пособие. – М.: Горячая линия–Телеком, 2020. – 120 с.

Перечень материально-технического обеспечения:

учебно-исследовательский стенд для изучения протокола XMPP (демонстрация), Linux-хост для демонстрации анализа сетевых пакетов, пакетные анализаторы WildPackets, CommView, Wireshark.

**Б.1.С.6.4. Дисциплина «Защита информационных процессов   
в телекоммуникационных сетях обеспечения функционирования летательных аппаратов»**

Коды формируемых компетенций: ОПК-6.2.

В результате изучения дисциплины студент должен

знать:

- типовые сетевые атаки и способы защиты от них;

- методы и средства контроля уровня безопасности информационных процессов в сетях обработки данных с летательных аппаратов;

уметь:

- применять программно-аппаратные средства защиты объектов аэрокосмического и наземного сегментов телекоммуникационной системы от несанкционированного доступа;

- применять методы задания базовых параметров и параметров защиты от несанкционированного доступа к операционным системам объектов наземного сегмента аэрокосмических телекоммуникационных систем

Примерное распределение часов: трудоемкость дисциплины 6 з.е., 216 час.

Форма контроля: экзамен

Содержание дисциплины:

**Типовые сетевые атаки на телекоммуникационные сети обеспечения функционирования летательных аппаратов**. Жизненный цикл сетевых атак. Атаки на наземный сегмент. Атаки на бортовые информационные системы. Атаки на канал передачи данных. Общая классификация сетевых атак на телекоммуникационные сети обеспечения функционирования летательных аппаратов. **Способы защиты от сетевых атак** Контроль и анализ трафика наземного и бортового сегмента. Анализ аномалий. Контроль и анализ защищённости наземного сегмента. Контроль параметров и работоспособности средств обработки данных. Аутентификация и идентификация, параметры протоколов передачи данных, используемые в задачах защиты информации. Удаленный доступ к программному обеспечению КА. **Защита от несанкционированного доступа к аэрокосмическому и наземному сегменту** Основные требования, определяющие выбор средств защиты информации. Криптографическая защита. Аутентификационные механизмы и факторы аутентификации. Методы контроля целостности программного обеспечения, в том числе микропрограмм. Структурно-функциональная схема системы защиты информации наземного сегмента телекоммуникационной системы, обеспечивающей функционирование КА. Структурно-функциональная схема системы защиты информации аэрокосмического сегмента телекоммуникационной системы, обеспечивающей функционирование КА. **Защита операционных систем наземного сегмента** Контроль целостности операционной системы. Доверенная загрузка. Аутентификационные механизмы операционных систем. Криптографическая подсистема. Модели и механизмы разграничения доступа. Контроль доступа к объектам операционной системы. Контроль доступа к памяти. Анализ работоспособности защитных механизмов.

Рекомендуемый перечень лабораторных работ:

1. Контроль и анализ защищенности наземного сегмента.

2. Анализ безопасности и типовые атаки на канал передачи информации.

3. Моделирование атак на бортовую аппаратуру.

4. Помехоустойчивость и оценка реальной помеховой обстановки для канала получения данных с КА

Рекомендуемый перечень основной литературы:

1. *Молотов Е.П.* Наземные радиотехнические системы управления космическими аппаратами. – М.: Физматлит, 2004. – 256 с.

2. Проектирование защищённых оптических телекоммуникационных систем : учебное пособие. / А.В. Горбунов, Ю.В. Зачиняев, А.П. Плёнкин. – Ростов-на-Дону; Таганрог: Южный федеральный университет, 2019. – 128 с.

3. *Кащеев Н.А.* Радиотехнические средства управления космическими аппаратами [Электронный ресурс]: учебное пособие. – М., 2005. – 202 с.

4. Методологические основы построения защищенных автоматизированных систем: учебное пособие. / А.В. Душкин, О.В. Ланкин, С.В. Потехецкий, А.П. Данилкин, А.А. Малышев. – Воронеж: ВГУИТ, 2013. – 263 с.

5. Бортовые системы управления космическими аппаратами: учебное пособие. / Бровкин А.Г., Бурдыгов Б.Г., Гордийко С.В. и др.; под редакцией А.С. Сырова. – М.: Изд-во МАИ-ПРИНТ, 2010.

Перечень материально-технического обеспечения:

- радиотехнические комплексы GR RASTA, GR CORTEX, National Instruments (LabVIEW), технические средства наземной станции управления;

- сканер защищенности (например, RedCheck или MaxPatrol).

**Б.1.С.6.5. Дисциплина «Методы защиты радиолиний аэрокосмических телекоммуникационных систем с использованием перспективных сигнально-кодовых конструкций»**

Коды формируемых компетенций: ОПК-6.3.

В результате изучения дисциплины студент должен

знать:

- назначение, типы и основные характеристики радиолиний аэрокосмических систем;

- методы и средства повышения скрытности использования радиолиний аэрокосмических систем;

- основные уязвимости радиоканалов аэрокосмических телекоммуникационных систем и методы их защиты;

уметь:

- формировать исходные данные и ограничения при проектировании аэрокосмических телекоммуникационных систем и сетей;

- разрабатывать энергетически эффективные инфокоммуникационные системы со скрытыми радиоканалами информационного взаимодействия;

владеть:

- приемами и методикой выполнения спектрального анализа сигнально-кодовых конструкций (СКК) для обеспечения энергетической и структурной скрытности в радиоканалах беспилотных летательных аппаратов (БПЛА).

Примерное распределение часов: трудоемкость дисциплины 6 з.е., 216 час.

Форма контроля: экзамен

Содержание дисциплины:

**Общие характеристики и методы защиты радиоканалов.** Назначение, типы радиолиний аэрокосмических телекоммуникационных систем и их особенности. Понятие о радиолиниях, радиоканалах. Общие характеристики. Особенности радиолиний, используемых аэрокосмическими объектами. Общие характеристики радиолиний, используемых аэрокосмическими объектами. **Общие источники уязвимостей радиоканалов** телекоммуникационных систем**.** Уязвимости и проблемы защиты радиоканалов телекоммуникационных систем. Объекты и методы защиты радиоканалов. Характеристики СКК, применяемых в радиолиниях командно-измерительных аэрокосмических систем. Характеристики СКК, применяемых в радиолиниях передачи информации и связи аэрокосмических систем. **Общие направления защиты радиоканалов.** Понятие о скрытности работы радиосистем. Типы скрытности. Методы и средства достижения структурной скрытности в асинхронно-адресных аэрокосмических ТКС. **Особенности защиты радиоканалов спутниковых систем.** Характеристики и особенности использования спутниковых радиоканалов. Особенности СКК, применяемых в радиоканалах спутниковых систем. Особенности применения энергетической и структурной скрытности в радиоканалах спутниковых систем. Характеристики и особенности СКК, применяемых в радиоканалах спутниковых систем. Методы энергетической и структурной скрытности в радиоканалах спутниковых систем. **Особенности защиты радиоканалов атмосферных летательных аппаратов.** Характеристики и особенности использования атмосферных радиоканалов. Особенности СКК, применяемых в радиоканалах БПЛА. Особенности применения энергетической и структурной скрытности в радиоканалах БПЛА. Характеристики помехоустойчивости и особенности СКК, применяемых в радиоканалах БПЛА. Методы энергетической и структурной скрытности в радиоканалах БПЛА.

Рекомендуемый перечень основной литературы:

1. Карпухин Е.О. Методы скрытой передачи информации: учебное пособие. – М.: Горячая линия–Телеком, 2020. – 80 с.

2. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: учебное пособие. / Под редакцией Ю.Ф. Каторина. – СПб: НИУ ИТМО, 2012. – 416 с.

3. Борисов В.И. и др. Помехозащищенность систем радиосвязи. – М.: Радиотехника, 2010.

Перечень материально-технического обеспечения:

компьютерный класс, оснащенный рабочими местами на базе вычислительной техники с установленным программным обеспечением, предназначенным для разработки и моделирования (LabVIEW, MATLAB или аналогичные им).

**Б.1.С.7.1. Дисциплина «Разработка аппаратного и программного обеспечения узлов и устройств защищенных телекоммуникационных систем»**

Коды формируемых компетенций: ОПК-7.1

В результате изучения дисциплины студент должен

знать:

- современную элементную базу компонентов защищенных телекоммуникационных систем;

- средства проектирования цифровых узлов и устройств защищенных телекоммуникационных систем на базе ПЛИС;

- функциональные возможности ПЛИС при разработке аппаратного и программного обеспечения типовых узлов и устройств защищенных телекоммуникационных систем;

уметь:

- проводить анализ компонентов защищенных телекоммуникационных систем на базе ПЛИС;

- выбирать архитектуры ПЛИС при разработке типовых узлов и устройств защищенных телекоммуникационных систем;

- учитывать требования информационной безопасности при разработке технического задания на аппаратное и программное обеспечение компонентов защищенных телекоммуникационных систем;

владеть:

- навыками работы с инструментальными средствами разработки узлов и устройств защищенных телекоммуникационных систем на базе ПЛИС.

Примерное распределение часов: трудоемкость дисциплины 4 з.е., 144 час.

Форма контроля: экзамен

Содержание дисциплины:

**Архитектура и схемотехника ПЛИС.** Элементная база устройств защищенных телекоммуникационных систем. Базовые матричные кристаллы (вентильные матрицы). Классификация логических микросхем программируемой логики. Сложные программируемые логические устройства CLPD. Программируемые пользователем вентильные матрицы FPGA. ПЛИС с комбинированной архитектурой. СБИС типа «система на кристалле» с однородной и блочной структурой. Способы оценки параметров ПЛИС. Функциональные возможности ПЛИС при разработке элементов защищенных телекоммуникационных систем. **Проектирование ПЛИС.** Основы организации проектной процедуры для ПЛИС. Схемотехническое проектирование ПЛИС. Проектирование ПЛИС на основе языков описания аппаратных средств. Проектирование на основе языков С/С++ и других языках. Структура и организация САПР. Основные этапы проектирования ПЛИС. Проблемы и методы проектирования СБИС типа «система на кристалле». **Языки описания аппаратуры.** Язык описания аппаратуры VHDL. Язык описания аппаратуры Verilog. **Проектирование цифровых устройств на базе ПЛИС фирмы Xilinx в среде WEBPACK ISE с учетом требований информационной безопасности.** Изучение архитектуры проекта, синтаксиса, типов данных и операций языка VHDL в среде WEBPACK ISE. Синтез проекта с использованием средств пакета WebPACK ISE. Функциональное моделирование проектируемого устройства на базе ПЛИС с использованием средств пакета WebPACK ISE. Средства программирования и отладки. Учет требований информационной безопасности.

Рекомендуемый перечень лабораторных работ:

1. Счетчики и их синтез в интегрированной среде WEBPACK ISE;

2. Разработка генератора псевдослучайной последовательности в интегрированной среде WEBPACK ISE;

3. Разработка модуля помехоустойчивого кодирования в интегрированной среде WEBPACK ISE.

Рекомендуемый перечень основной литературы:

1. Ушенина И.В. Проектирование цифровых устройств на ПЛИС: учебное пособие. – СПб.: Лань, 2019. – 408 с.

2. Язык verilog и проектирование цифровых устройств на ПЛИС: учебно-методическое пособие. / Е. В. Богатиков, А. Н. Шебанов. – Воронеж: ВГУ, 2018. –   
61 с.

3. Наваби З. Проектирование встраиваемых систем на ПЛИС. / Перевод с английского В.В. Соловьева. – Москва: ДМК Пресс, 2016. – 464 с.

4. Максфилд К. Проектирование на ПЛИС. Курс молодого бойца: учебное пособие. – М.: Лань, 2010. – 407 с.

5. Бобрешов А.М., Дыбой А.В. Проектирование цифровых устройств на базе ПЛИС фирмы XILINX в среде WebPACK ISE: Учебно-методическое пособие. – Воронеж: Изд-во ВГУ, 2004. – 51 с.

Перечень материально-технического обеспечения:

интегрированная среда разработки ISE WEBPACK.

**Б.1.С.7.2. Дисциплина «Управление информационной безопасностью телекоммуникационных систем»**

Коды формируемых компетенций: ОПК-7.2.

В результате изучения дисциплины студент должен

знать:

- процессы и методы планирования системы управления информационной безопасностью телекоммуникационных систем;

- основные методы идентификации, анализа, оценивания и обработки рисков;

- процессы и методы поддержки и функционирования системы управления информационной безопасностью телекоммуникационных систем;

- процессы и методы проверки функционирования и совершенствования системы управления информационной безопасностью телекоммуникационных систем;

уметь:

- определять и обосновывать активы, ресурсы, роли для процессов системы управления информационной безопасностью телекоммуникационных систем;

- определять возможность применения соответствующего математического аппарата при использовании количественных и качественных методов оценки рисков;

владеть:

- навыками формирования и описания процессов системы управления информационной безопасностью телекоммуникационных систем.

Примерное распределение часов: трудоемкость дисциплины 9 з.е., 324 час.

Форма контроля: зачет, экзамен

Содержание дисциплины:

**Процессы планирования системы управления информационной безопасностью телекоммуникационной системы.** Управление рисками информационной безопасности. Политика информационной безопасности телекоммуникационной системы. **Процессы поддержки и функционирования системы управления информационной безопасностью телекоммуникационной системы.** Реализация защитных мер. Обучение персонала и сотрудников информационной безопасности. Управление изменениями телекоммуникационной системы. Управление инцидентами информационной безопасности. **Процессы проверки функционирования системы управления информационной безопасностью телекоммуникационной системы.** Мониторинг информационной безопасности. Проверка соответствия информационной безопасности телекоммуникационной системы. Аудит информационной безопасности телекоммуникационной системы. Совершенствование системы управления информационной безопасностью телекоммуникационной системы. **Теория риска.** Опасности, виды опасностей; риск как опасность; риск как неопределенность; риск как возможность; виды рисков; рискообразующие факторы; угроза, уязвимость, ущерб; человеческий фактор; опасные действия; надежность сотрудников; способы оценки надежности работников; процессы управления риском; идентификация риска, анализ и оценивание риска; обработка риска; принятие риска; коммуникация риска; мониторинг и пересмотр риска*.*

Рекомендуемый перечень основной литературы:

1. Обеспечение информационной безопасности бизнеса. / В.В. Андрианов, С.Л. Зефиров, В.Б. Голованов, Н.А. Голдуев; под ред. А.П. Курило – М.: Издательство Альпина Паблишерз, 2011. – 373 с.

2. Уродовских В.Н. Управление рисками предприятия [Электронный ресурс]: учебное пособие. – М.: Вузовский учебник: ИНФРА-М, 2011. – 168с.

3. Шапкин А.С., Шапкин В.А. Теория риска и моделирование рисковых ситуаций [Электронный ресурс]: учебник. – М.: Издательско-торговая корпорация «Дашков и К», 2009. – 880с.

**Б.1.С.7.3. Дисциплина «Защита программных средств защищенных телекоммуникационных систем»**

Коды формируемых компетенций: ОПК-7.3

В результате изучения дисциплины студент должен

знать:

- принципы работы инструментальных средств исследования программного обеспечения защищенных телекоммуникационных систем;

- принципы и средства защиты программного обеспечения защищенных телекоммуникационных систем;

уметь:

- выявлять уязвимости защиты программных средств защищенных телекоммуникационных систем и находить пути их устранения;

- проектировать и реализовывать защиту программных средств защищенных телекоммуникационных систем, исходя из поставленных целей защиты;

владеть:

- навыками работы с инструментальными средствами для исследования программных средств защищенных телекоммуникационных систем.

Примерное распределение часов: трудоемкость дисциплины 4 з.е., 144 час.

Форма контроля: экзамен

Содержание дисциплины:

**Угрозы программному обеспечению защищенных телекоммуникационных систем.** Уязвимости программного обеспечения защищенных телекоммуникационных систем. Методы исследования программного обеспечения. Принципы работы отладчиков. Классификация отладчиков. **Принципы работы дизассемблеров.** Методика исследования программного обеспечения с помощью отладчиков и дизассемблеров. Защиты программного обеспечения от исследования. **Защита программного обеспечения от несанкционированного копирования.** Защита программного обеспечения от исследования и модификации.

Рекомендуемый перечень лабораторных работ:

1. Исследование программного обеспечения с использованием отладчиков.

2. Исследование программного обеспечения с использованием дизассемблеров.

3. Защита программного обеспечения от исследования и отладки.

4. Защита программного обеспечения от несанкционированного копирования.

Рекомендуемый перечень основной литературы:

1. Защита от хакеров коммерческого сайта [Электронный ресурс]: учебное пособие. / Р. Рассел и др. – Электрон. Дан. – М.: ДМК Пресс, 2009. – 552 с.

2. *Фостер Д.* Защита от взлома: сокеты, эксплойты, shell-код [Электронный ресурс] – Электрон. Дан. – М.: ДМК Пресс, 2008. – 784 с.

Перечень материально-технического обеспечения:

программное обеспечение: дизассемблер, отладчик, hex-редактор.

**Б.1.С.8.1. Дисциплина «Системы радиосвязи и сети телерадиовещания»**

Коды формируемых компетенций: ОПК-8.1.

В результате изучения дисциплины студент должен

знать:

- теоретические основы частотно-временного и кодового планирования сетей радиосвязи и телерадиовещания;

- принципы и методы частотного планирования сетей телерадиовещания;

уметь:

- выбирать методы частотно-временного и кодового планирования сетей радиосвязи и телерадиовещания;

- применять технологии частотно-временного и кодового планирования для разработки сетей радиосвязи и телерадиовещания;

владеть:

- инструментарием решения вопросов выделения частот каналов для развития сетей радиосвязи и телерадиовещания.

Примерное распределение часов: трудоемкость дисциплины 9 з.е., 324 час.

Форма контроля: экзамен.

Содержание дисциплины:

**Принципы построения систем радиосвязи и телерадиовещания.** Регламент радиосвязи РФ. Стандарты аналоговых и цифровых систем радиосвязи и телерадиовещания. Принципы частотно-временного планирования. **Радиорелейные линии связи прямой видимости.** Системы цифровой радиорелейной связи. Автоматизация проектирования цифровых радиорелейных линий. Частотно-временное и кодовое планирование радиорелейной связи. **Системы подвижной радиосвязи.** Транкинговые системы радиосвязи. Стандарты аналоговой и цифровой транкинговой радиосвязи. Системы сотовой связи 2, 3, 4 и 5 поколений. Частотно-временное и кодовое планирование в системах сотовой связи. Стандарты кодирования в пейджинговой связи. **Спутниковые системы радиосвязи и телерадиовещания.** Современные спутниковые системы связи. Спутниковые системы персональной радиосвязи. Частотно-временное и кодовое планирование в системах спутниковой радиосвязи и телерадиовещания. **Глобальные информационные сети на базе систем подвижной радиосвязи третьего и четвертого поколений.** Беспроводные локальные сети на основе стандартов IEEE 802.11. Персональные сети радиодоступа. Стандарты IEEE 802.15, Bluetooth. Стандарты городских сетей широкополосного радиодоступа IEEE802.16 (WiMAX), LTE.

Рекомендуемый перечень основной литературы:

1. Голиков А. Системы радиосвязи и сети телерадиовещания: Курс лекций, компьютерный практикум, задание на самостоятельную работу. – Томск, 2018. –   
354 с.

2. Вершинин А.С., Эрдынеев Ж.Т. Космические и наземные системы радиосвязи и сети телерадиовещания: учебное пособие. – Томск, 2013. – 184 с.

3. [Варгаузин](https://www.elibrary.ru/author_items.asp?refid=614024044&fam=%D0%92%D0%B0%D1%80%D0%B3%D0%B0%D1%83%D0%B7%D0%B8%D0%BD&init=%D0%92+%D0%90) В.А., [Цикин](https://www.elibrary.ru/author_items.asp?refid=614024044&fam=%D0%A6%D0%B8%D0%BA%D0%B8%D0%BD&init=%D0%98+%D0%90) И.А. Методы повышения энергетической и спектральной эффективности цифровой радиосвязи: учебное пособие. – СПб.: БХВ-Петербург, 2013. – 352 с.

4. Тищенко А.Б. Многоканальные телекоммуникационные системы. Ч.1. Принципы построения телеком. систем с времен. раздел. каналов: учебное пособие. – М.: ИЦ РИОР: НИЦ ИНФРА-М, 2013 – 104 с.

5. Технологии мобильной связи: услуги и сервисы. / А.Г. Бельтов, И.Ю. Жуков, Д.М. Михайлов, А.В. Стариковский. – М.: НИЦ ИНФРА-М, 2013. – 206 с.

**Б.1.С.8.2. Дисциплина «Устройства приема и обработки сигналов   
в защищенных системах радиосвязи»**

Коды формируемых компетенций: ОПК-8.2.

В результате изучения дисциплины студент должен

знать:

- теоретические основы приема, передачи и обработки сигналов в целях обеспечения эффективности и защищенности систем радиосвязи и телерадиовещания;

- основные понятия и принципы защиты информации в системах радиосвязи и телерадиовещания;

уметь:

- использовать методы повышения помехозащищенности систем телерадиовещания;

- анализировать системы радиосвязи на предмет защищенности;

владеть:

- навыками решения типовых задач повышения эффективности и защищенности систем радиосвязи и телерадиовещания.

Примерное распределение часов: трудоемкость дисциплины 9 з.е., 324 час.

Форма контроля: экзамен.

Содержание дисциплины:

**Назначение и виды устройств приема и обработки сигналов.** Структурные схемы и принцип действия. Основные характеристики. **Входные цепи устройств приема.** Назначение, характеристики и виды входных цепей. Анализ одноконтурной входной цепи. Входные цепи при работе с настроенной антенной. Входные цепи при работе с ненастроенной антенной. Особенности построения входных цепей приемников различных диапазонов волн. **Усилители радиосигналов.** Назначение, основное характеристики и схемы усилителей на независимых элементах. Анализ обобщенной эквивалентной схемы усилителя радиочастоты. Влияние внутренней обратной связи. Условия устойчивости работы усилителя. Диапазонный резонансный усилитель. Малошумящие усилители СВЧ. Полосовые усилители промежуточной частоты. **Преобразователи частоты.** Назначения и классификация. Общая теория преобразования на независимом электронном приборе. Особенности транзисторных преобразователей частоты различных диапазонов волн. Диодный и емкостной преобразователи частоты. Гетеродины. **Детекторы радиосигналов.** Назначение, классификация и основные характеристики амплитудных детекторов. Общая теория детектирования амплитудно-модулированных сигналов. Цифровые детекторы АМ сигналов. Детекторы угловой модуляции и амплитудные ограничители. Виды фазовых детекторов. Цифровой фазовый детектор. Квадратурный фазовый детектор. Общая теория частотного детектирования. Виды частотных детекторов. Принципы построения цифровых частотных детекторов. Демодуляторы мобильных систем связи. **Регулировки в радиоприемниках.** Назначение и виды регулировок. Автоматическая регулировка усиления. Автоматическая подстройка радиочастоты. Фазовая автоподстройка частоты. Применение ФАПЧ в синтезаторах частоты. Применение микропроцессоров для контроля и управления приемников. **Особенности построения устройств приема в защищенных системах радиосвязи.** Приемные устройства радиорелейных систем и систем спутниковой связи и вещания. Приемники звукового и телевизионного вещания. Приемники систем персонального радиовызова.

Рекомендуемый перечень лабораторных работ:

1. Исследование входной цепи.

2. Изучение преобразования частоты в супергетеродинном приемнике.

3. Изучение программно-определяемого радио.

4. Изучение формирования импульсов в цифровой связи.

Рекомендуемый перечень основной литературы:

1. Галочкин В.А. Устройства приема и обработки сигналов. Учебное пособие (конспект лекций). – Самара: ФГОБУ ВПО ПГУТИ, 2015. – 425 с.

2. Пушкарёв В.П. Устройства приема и обработки сигналов [Электронный ресурс]: Учебное пособие. – 2012. – 201 с. – Режим доступа: https://edu.tusur.ru/training/publications/1519.

3. Шостак А.С. Прием и обработка сигналов. Часть 1 [Электронный ресурс]: Курс лекций. – 2012. – 161 с. – Режим доступа: https://edu.tusur.ru/training/publications/1220.

4. Шостак А.С. Прием и обработка сигналов. Часть 2 [Электронный ресурс]: Курс лекций. – 2012. – 87 с. – Режим доступа: https://edu.tusur.ru/training/publications/1222.

**Б.1.С.8.3. Дисциплина «Защита информации в системах радиосвязи   
и телерадиовещания»**

Коды формируемых компетенций: ОПК-8.3.

В результате изучения дисциплины студент должен

знать:

- принципы и стандарты построения систем, сетей и устройств защищенной радиосвязи и телерадиовещания;

- технологии создания систем, сетей и устройств защищенной радиосвязи и телерадиовещания;

уметь:

- разрабатывать системы, сети и устройств защищенной радиосвязи и телерадиовещания;

решать типовые задачи по проектированию защищенных сетей радиосвязи и телерадиовещания;

владеть:

- базовыми навыками решения типовых задач создания систем, сетей и устройств защищенной радиосвязи и телерадиовещания.

Примерное распределение часов: трудоемкость дисциплины 9 з.е., 324 час.

Форма контроля: экзамен.

Содержание дисциплины:

**Комплексный анализ защищенности и инструментальный мониторинг ведомственных телевизионных систем (ТВС).** Проектирование и оценка надежности результатов разработки программных элементов ТВС. Эксплуатация программно-аппаратных средства защиты ТВС с учетом специфики угроз информации в них. **Проблемы контроля безопасности информации в телекоммуникационных системах органов государственного управления.** Обоснование структуры системы комплексного контроля безопасности информации.

Рекомендуемый перечень основной литературы*:*

1. Шаньгин В.Ф. Комплексная защита информации в корпоративных сетях: учебное пособие. – М.: Форум-Инфра-М, 2013.

2.  Модели и методы повышения живучести современных систем связи [Электронный ресурс]. / Величко В.В., Попков Г.В., Попков В.К. – Электрон, текстовые данные. – М.: Горячая линия-Телеком, 2014. – 270 с.

3. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие. / Башлы И.И., Бабаш А.В., Баранова Е.К. – Электрон, текстовые данные. – М.: Евразийский открытый институт, 2012. – 311 с.

4. Аверченков А.В. и др. Разработка системы технической защиты информации. – Брянск: БГТУ, 2012.

5. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс]. – Электрон, текстовые данные. – М.: ДМК Пресс, 2014. –   
702 с.

6. Организационная защита информации [Электронный ресурс]: учебное пособие для вузов. / Аверченков В.И., Рытов М.Ю. – Электрон, текстовые данные. – Брянск: Брянский государственный технический университет, 2012. – 184 с.

7. Аверченков В.И. Аудит информационной безопасности [Электронный ресурс]: учебное пособие для вузов. – Электрон, текстовые данные. – Брянск: Брянский государственный технический университет, 2012. – 268 с.

8. Методы и средства инженерно-технической защиты информации [Электронный ресурс]: учебное пособие. / В.И. Аверченков [и др.]. – Электрон, текстовые данные. – Брянск: Брянский государственный технический университет, 2012. – 187 с.

**Б.1.С.9.1. Дисциплина «Менеджмент информационной безопасности телекоммуникационных систем и сетей»**

Коды формируемых компетенций: ОПК-9.1.

В результате изучения дисциплины студент должен

знать:

- основные методы управления информационной безопасностью телекоммуникационных систем и сетей;

- методику выработки и реализации управленческих решений по обеспечению защиты телекоммуникационных систем и сетей;

- цели и задачи управления персоналом по обеспечению защиты телекоммуникационных систем и сетей;

уметь:

- определять угрозы, реализация которых может привести к нарушению безопасности и корректности функционирования телекоммуникационных систем и сетей;

- разрабатывать политику безопасности телекоммуникационных систем и сетей;

- производить постановку задач персоналу по обеспечению защиты телекоммуникационных систем и сетей;

владеть:

- навыками оценки рисков, связанных с осуществлением угроз безопасности телекоммуникационных систем и сетей.

Примерное распределение часов: трудоемкость дисциплины 6 з.е., 216 час.

Форма контроля: экзамен.

Содержание дисциплины:

**Анализ телекоммуникационных систем и сетей как объектов защиты.** Технологии анализа объекта защиты. Типы информационных систем. Методы оценки ущерба от реализации угроз информационной безопасности; комплекс стандартов в области управления информационной безопасности (ГОСТ Р ИСО/МЭК 27000). Модель угроз и модель нарушителя. Подходы к формированию модели нарушителя и модели угроз. Требования регуляторов к формированию модели нарушителя и модели угроз телекоммуникационных систем и сетей. **Оценка рисков информационной безопасности.** Основные положения стандартов в области управления рисками информационной безопасности. Система управления информационной безопасностью телекоммуникационных систем и сетей. Основные положения стандартов по проектированию, реализации и аудиту системы управления информационной безопасностью. **Организация управления персоналом в контексте обеспечения информационной безопасности телекоммуникационных систем и сетей.** Политика информационной безопасности. Основные положения стандартов в области регламентации обеспечения информационной безопасности. Управление инцидентами информационной безопасности. Основные положения стандартов в области управления инцидентами информационной безопасности. Регламентация действий сотрудников при возникновении нештатных ситуаций.

Рекомендуемый перечень лабораторных работ:

1. Анализ рисков информационной безопасности на основе построения модели информационных потоков.

2. Анализ рисков на основе модели угроз и уязвимостей.

3. Анализ рисков на основе международных стандартов ISO 27002 и 27005.

Рекомендуемый перечень основной литературы:

1. Основы управления информационной безопасностью. Серия «Вопросы управления информационной безопасностью. Выпуск 1». – 2-е изд., испр.: учебное пособие для вузов. / А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия- Телеком, 2016. – 244 с.

Перечень материально-технического обеспечения:

система автоматизации оценки рисков информационной безопасности.

**Б.1.С.9.2. Дисциплина «Правила и процедуры по обеспечению информационной безопасности телекоммуникационных систем и сетей»**

Коды формируемых компетенций: ОПК-9.2.

В результате изучения дисциплины студент должен

знать:

- содержание и порядок деятельности персонала при вводе в эксплуатацию (выводе из эксплуатации) телекоммуникационных систем и сетей;

- содержание и порядок деятельности персонала при эксплуатации телекоммуникационных систем и сетей;

- содержание и порядок деятельности персонала по выявлению и реагированию на инциденты информационной безопасности;

уметь:

- определять правила и процедуры защиты информации при вводе в эксплуатацию (выводе из эксплуатации) телекоммуникационных систем и сетей;

- определять правила и процедуры защиты информации при эксплуатации телекоммуникационных систем и сетей;

- определять правила и процедуры выявления и реагирования на инциденты информационной безопасности.

Примерное распределение часов: трудоемкость дисциплины 5 з.е., 180 час.

Форма контроля: экзамен.

Содержание дисциплины:

**Жизненный цикл телекоммуникационных систем и сетей.** Правила и процедуры защиты информации на этапах жизненного цикла телекоммуникационных систем и сетей. **Система управления инцидентами информационной безопасности.** Обнаружение событий информационной безопасности и инцидентов информационной безопасности и оповещение о них. Реагирование на инциденты информационной безопасности. **Безопасность, связанная с персоналом.** Правила и условия работы. Осведомленность, обучение и практическая подготовка персонала в области информационной безопасности.

**Б.1.С.9.3. Дисциплина «Обеспечение устойчивости телекоммуникационных систем и сетей»**

Коды формируемых компетенций: ОПК-9.2.

В результате изучения дисциплины студент должен

знать:

- типы, основные характеристики средств измерений и контроля процесса и параметров функционирования телекоммуникационных систем и сетей;

- способы организации, методики, нормативные требования и содержание технического обслуживания телекоммуникационных систем и сетей;

- методики и нормативные требования к действиям в целях восстановления процесса и параметров функционирования телекоммуникационных систем и сетей;

уметь:

- проводить текущий контроль показателей и процесса функционирования телекоммуникационных систем и сетей, предусмотренный регламентом их эксплуатации;

- проводить предусмотренные регламентом работы по восстановлению процесса и параметров функционирования телекоммуникационных систем и сетей;

владеть:

- навыками восстановления процесса функционирования после сбоев и отказов телекоммуникационных систем и сетей.

Примерное распределение часов: трудоемкость дисциплины 3 з.е., 108 час.

Форма контроля: зачет.

Содержание дисциплины:

**Уровень сервиса обслуживания (QoS).** Рабочие модели QoS. Функциональная модель информационно-телекоммуникационной сети. **Оценка стратегии комплексного информационного воздействия на телекоммуникационные системы и сети.** Оценки опасности компьютерных атак на телекоммуникационные системы и сети. Методика оценки стратегии информационного воздействия на телекоммуникационные системы и сети. **Устойчивость телекоммуникационных систем и сетей в условиях воздействия компьютерных атак.** Методика оценки устойчивости в условиях воздействия компьютерных атак. Синтез системы защиты информационно-телекоммуникационной сети. Направления повышения защищенности телекоммуникационных систем и сетей. **Оценка эффективности средств защиты телекоммуникационных систем и сетей от атак.** Методика синтеза системы защиты телекоммуникационных систем и сетей в условиях воздействия компьютерных атак.

Рекомендуемый перечень основной литературы:

1. Надежность информационных систем: Учебник для вузов ж.-д. транспорта. – М.: ГОУ «Учебно-методический центр по образованию на железнодорожном транспорте», 2007. – 318 с.

**Б.1.С.9.4. Дисциплина «Мониторинг безопасности телекоммуникационных систем и сетей»**

Коды формируемых компетенций: ОПК-9.3.

В результате изучения дисциплины студент должен

знать:

- методы контроля функционирования телекоммуникационных систем и сетей;

- принципы построения систем обнаружения компьютерных атак;

- методы обработки данных мониторинга безопасности телекоммуникационных систем и сетей;

уметь:

- применять средства мониторинга работоспособности и эффективности применяемых средств защиты телекоммуникационных систем и сетей;

- применять инструментальные средства проведения мониторинга защищенности сетевых ресурсов телекоммуникационных систем и сетей;

- составлять отчеты по результатам проверок защищенности телекоммуникационных систем и сетей;

владеть:

- навыками анализа защищенности телекоммуникационных систем и сетей с использованием сканеров безопасности и средств автоматического реагирования на попытки несанкционированного доступа.

Примерное распределение часов: трудоемкость дисциплины 6 з.е., 216 час.

Форма контроля: экзамен.

Содержание дисциплины:

**Нормативная база и основы мониторинга безопасности телекоммуникационных систем и сетей.** Обзор международных и российских стандартов, регламентирующих мониторинг безопасности. Принципы непрерывности. **Построение системы мониторинга.** Принципы и критерии выбора параметров мониторинга. Подходы к построению мониторинга. Мониторинг с участием агентов и мониторинг при помощи конечных агентов. Иерархии систем мониторинга. Протоколы мониторинга телекоммуникационных систем и сетей. Инструменты для осуществления мониторинга. **Организация системы мониторинга безопасности.** Разбор существующих систем мониторинга, их сильные и слабые стороны. Документальное оформление процедуры мониторинга. Описание инструкции реагирование на инциденты (плейбук). Организация мониторинга безопасности телекоммуникационных систем и сетей.

Рекомендуемый перечень лабораторных работ:

1. Работа с протоколами мониторинга. Мониторинг без участия агентов. Анализ работы протокола SNMP.

2. Процессный подход к организации мониторинга. Цикл непрерывности. Выбор критериев мониторинга для необходимы для непрерывности процессов.

3. Мониторинг при помощи агентов. Установка и настройка системы мониторинга Zabbix.

4. Работа с подсистемой WMI. Подключение хостов к системе мониторинга Zabbix. Настройка дашбордов для команды мониторинга.

5. Развертывание SIEM системы. Определение источников получения информации о событиях информационной безопасности. Разбор необходимости нормализации событий. Создание правил корреляции событий. Создание инцидентов на основе событий информационной безопасности

6. Методы хранения и анализа собранной информации. Формирование дашбордов в системах с открытым исходным кодом.

Перечень материально-технического обеспечения:

- система мониторинга Zabbix;

- SIEM система;

- системы хранения и анализа собранной информации (Prometheus, Grafana, InfluxDB).

**Б.1.С.10.1. Дисциплина «Квантовая криптография в телекоммуникационных системах и сетях транспорта»**

Коды формируемых компетенций: ОПК-10.1.

В результате изучения дисциплины студент должен

знать:

- основные принципы квантовых вычислений и квантовой связи, используемые в задачах криптографии;

- квантовые коммуникации (квантовое распределение ключей);

- принципы квантово-криптографической защиты высокоскоростных оптических линий связи;

- постквантовые алгоритмы и принципы оптических измерений в телекоммуникационных системах и сетях транспорта;

уметь:

- формулировать предложения по вопросам обеспечения информационной безопасности с использованием квантовой криптографии в телекоммуникационных системах на транспорте;

- проводить исследование уязвимостей и разрабатывать модели оценки телекоммуникационных систем, построенных на технологиях квантовой криптографии и квантовых сетей;

владеть:

- методиками расчета и оценки эффективности защиты с использованием квантовой криптографии в телекоммуникационных систем и сетях на транспорте.

Примерное распределение часов: трудоемкость дисциплины 8 з.е., 288 час.

Форма контроля: экзамен

Содержание дисциплины:

**Основные принципы квантовых вычислений и квантовой связи, используемых в задачах криптографии.** Общие представления о методах криптографии и криптоанализа, основанные на фундаментальных законах квантовой физики. **Технологии квантового распределения ключей.** Анализ технологии квантовой криптографии и квантовых сетей в телекоммуникационных системах и сетях транспорта. Архитектура квантовых коммуникационных сетей. Схема практической реализации квантовой криптографии. Средства защиты высоконагруженных каналов связи транспорта. Система квантового распределения ключей на боковых частотах модулированного излучения. Высокопроизводительный шифратор с квантовым каналом распределения (обновления) криптографических ключей. **Принципы квантово-криптографической защиты высокоскоростных оптических линий связи (ВсОЛС).** Квантовая защита для волоконно-оптических линий связи. Оптические направляющие среды передачи (ОНСП). Основы теории. Принципы построения высокоскоростных оптических линий связи. Характеристики высокоскоростных оптических линий связи. Защита трафика служб голосовой и видеосвязи в сетях TCP/IP. Специализированные ВсОЛС в локальных и корпоративных сетях и системах транспорта. Обеспечение одновременной работы с ресурсами разных сегментов корпоративной сети, эффективность дистанционного тестирования. **Постквантовые алгоритмы и принципы оптических измерений в телекоммуникационных системах и сетях транспорта.** Уязвимости квантовых систем, в том числе на транспорте. Алгоритм исправления ошибок в квантовом канале. Постквантовые алгоритмы. Принципы оптических измерений в телекоммуникационных системах и сетях транспорта. Модели оценки рисков телекоммуникационных систем, построенных на технологиях квантовой криптографии и квантовых сетей. Модели оценки рисков ТКС в транспортных системах при использовании AI-технологий. Алгоритм качественного метода оценки рисков информационной безопасности.

Рекомендуемый перечень лабораторных работ:

1. Моделирование ли оценки рисков телекоммуникационных систем, построенных на технологиях квантовой криптографии и квантовых сетей;

2. Построение модельного алгоритма и расчет характеристик экспериментальной установки, влияющих на эффективность выбранного алгоритма;

3. Изучение методики измерения оптических потерь в телекоммуникационных систем и системах транспорта (по видам);

4. Определение места и характера повреждения оптического кабеля с использованием оптического рефлектометра;

5. Измерение полных и погонных потерь с использованием оптического рефлектометра.

Рекомендуемый перечень основной литературы:

1. [Граймс Роджер А.](https://www.labirint.ru/authors/230755/) [Апокалипсис криптографии. Подготовка криптографии к квантовым вычислениям](https://www.labirint.ru/books/823072/). – Изд-во ДМК-Пресс, 2021. – 286 с.

2. Квантовая криптография. Идеи и практика. – Изд-во Беларусская наука, 2007.

3. Фергюсон Н., Шнайер Б. Практическая криптография. – Изд-во Вильсон, 2005.

4. Бернхард Крис. Квантовые вычисления для настоящих айтишников. – Изд-во Питер, 2020.

5. М. Нильсен, И. Чанг Квантовые вычисления и квантовая информация. – Изд-во Мир, 2006.

6. Листвин А.В., Листвин В.Н. Рефлектометрия оптических волокон. – М.: ЛЕСАРарт, 2005.

Перечень материально-технического обеспечения:

оборудование: ViPNet Client 4U for Linux , модуль – практикум по волоконно-оптическим линиям связи – Плата (Тип-4) Emona Optics - Trainer 211;

- рефлектометр FTB-7000;

- оптические тестеры FTB-200 и FLS-600.

**Б.1.С.10.2. Дисциплина «Информационная безопасность и защита информации в интегрированных телекоммуникационных и корпоративных сетях транспорта»**

Коды формируемых компетенций: ОПК-10.2.

В результате изучения дисциплины студент должен

знать:

- информационную структуру сетей транспорта как объекта защиты;

- информационные ресурсы сетей транспорта как объекта защиты;

- критерии оценки защищенности телекоммуникационных систем и систем транспорта;

уметь:

- использовать программно-аппаратные методы защиты информации телекоммуникационных систем и сетей транспорта;

- использовать криптографические методы защиты информации телекоммуникационных систем и сетей транспорта;

владеть:

- навыками работы с программно-аппаратными средствами обеспечения информационной безопасности телекоммуникационных систем и сетей транспорта.

Примерное распределение часов: трудоемкость дисциплины 9 з.е., 324 час.

Форма контроля: экзамен.

Содержание дисциплины:

**Сетевые аномалии. Обнаружение, локализация, прогнозирование.** Методы, системы и инструменты анализа сетевых аномалий. Классификация методов, состав систем и инструментов сетевых аномалий. Анализ и мониторинг сетевого трафика. Сетевые анализаторы трафика, контроль сетевых устройств. Сетевая томография. Обнаружение и локализация аномалий объема. Обнаружение и локализация аномалий в крупномасштабной сети. Обнаружение и прогнозирование аномалий в потоковых данных. Обнаружение аномалий на основе прогнозирования профиля нормального функционирования. **Защита беспроводных сетей.** Защита локальной беспроводной сети стандарта IEEE 802.11. Уязвимости и уровни защиты беспроводных сетей. Аномалии сетевой безопасности. Защита сетей стандартов 5G, 6G. Уровни безопасности, основные угрозы, проблемы интеграции сетей передачи сотовых данных. Статистические характеристики трафика с DoS атакой. **Центры управления сетевой безопасностью в информационно-телекоммуникационных сетях и системах транспорта.** Анализ состояния обеспечения информационной безопасности информационно-телекоммуникационных сетей и систем транспорта. Информационно-телекоммуникационная сеть и системы транспорта как симбиоз телекоммуникационной и информационной сетей. Статистические характеристики аномальных вторжений. Исследование и разработка процессов обеспечения информационной и сетевой безопасности информационно-телекоммуникационных сетей и систем транспорта. Понятие обеспечения информационной безопасности информационно-телекоммуникационной сети. Проверка информационной безопасности информационно-телекоммуникационной сети как средство постоянного контроля общего управления информационной безопасностью на транспорте. Уязвимости, угрозы, сетевые атаки и инциденты для информационно-телекоммуникационных сетей и систем транспорта. Таксономия понятий уязвимости, угроз, сетевых атак и инцидентов информационной безопасности, в том числе в ТКС и системах транспорта. Обнаружение аномалий методами ДВП в режиме off-line. Анализ существующих Центров и выработка требований к Центрам интеллектуального управления сетевой безопасностью на транспорте. Понятие SIEM-системы. Эволюция Центров управления безопасностью. Построение типового Центра интеллектуального управления сетевой безопасностью для информационно-телекоммуникационной сети и систем транспорта. Методология и принципы построения типового Центра интеллектуального управления сетевой безопасностью. Обнаружение и классификация сетевых атак методами машинного обучения. Обнаружение компьютерных атак с применением нейронных сетей.

Рекомендуемый перечень лабораторных работ*:*

1. Разработка модели обнаружения аномалий в HTTP запросах.

2. Исследование критериев аномальных вторжений и сетевых атак.

3. Отбор числа и состава информативных признаков с использованием программных средств.

4. Бинарная классификация атак на примере базы данных UNSW-NB15/

Рекомендуемый перечень основной литературы:

1. Карпухин Е.О. Технологии и методы защиты инфокоммуникационных систем и сетей: учебное пособие. – М.: Горячая линия-Телеком, 2020. – 120 с.

2. Милославская Н.Г. Научные основы построения центров управления сетевой безопасностью в информационно-телекоммуникационных сетях. 2021.

3. Шелухин О.И. Сакалема Д.Ж., Филинова А.С. Обнаружение вторжений в компьютерные сети (сетевые аномалии): учебное пособие. – М.: Горячая линия-Телеком, 2018. – 220 с.

4. Шелухин О.И. Сетевые аномалии. Обнаружение, локализация, прогнозирование. – М.: Горячая линия-Телеком, 2020. – 448 с.

5. Классификация IP-трафика методами машинного обучения. / Шелухин О.И., Ерохин С.Д., Ванюшина А.В.; под ред. профессора О.И. Шелухина. – М.: Горячая линия-Телеком, 2018. – 284 с.

Перечень материально-технического обеспечения:

программный сниффер Wireshark, Iris Network Traffic Analyzer.

**Б.1.С.10.3. Дисциплина «Специальные измерения и техническая диагностика в защищенных сетях транспорта»**

Коды формируемых компетенций: ОПК-10.3.

В результате изучения дисциплины студент должен

знать:

- структуру и характеристики средств технического диагностирования и контроля, используемых в защищенных системах и сетях транспорта;

- основные технические характеристикиконтрольно-измерительных приборов параметров телекоммуникационных систем и сетей транспорта;

- основные положения национальных, межгосударственных и международных стандартов в части телекоммуникационных систем и сетей транспорта;

уметь:

- использовать и приборы общего и специального назначения для оценки функционального состояния телекоммуникационных систем и сетей транспорта;

- осуществлять выбор совокупности параметров для определения работоспособности защищенной телекоммуникационной системы транспорта;

- осуществлять оценку технических возможностей систем и сетей передачи информации при аттестации телекоммуникационных систем транспорта учётом требований по защите информации;

владеть:

- методами прогнозирования технического состояния средств защиты информации телекоммуникационных систем и защищенной телекоммуникационной системы транспорта;

- навыками работы со средствами и системами тестирования телекоммуникационных систем на транспорте (по видам транспорта).

Примерное распределение часов: трудоемкость дисциплины 10 з.е., 360 час.

Форма контроля: экзамен

Содержание дисциплины:

**Техническое диагностирования и контроль состояния ЗТКС.** Основные задачи технического диагностирования и контроля. Классификация СрДК. Виды и методы контроля. Особенности ЗТКС как объектов контроля. Основные контролируемые параметры. Методология как внутренняя технология измерений. Предпосылки использования средств диагностики и контроля ЗТКС. Система технического диагностирования и контроля. Выбор допусков на диагностические параметры. Поиск места отказа в ТКС и средствах защиты информации. Процесс и задачи технического обслуживания. Особенности технического диагностирования 3ТКС. Типы отказов оборудования. **Модели объектов технического диагностирования.** Функциональные состояния ЗТКС. Случайные процессы как инструмент описания градаций состояния ЗТКС. Диагностические модели: аналитические, графоаналитические, информационно-диагностические. Локализация места отказа ЗТКС по критерию «время-безотказность». Метод ветвей и границ. Метод половинных разбиений. Оптимизация алгоритма ПМО на основе информационного подхода. Прогнозирование состояния ЗТКС как обязательный инструмент перехода к технической эксплуатации по состоянию. Аналитическое прогнозирование. Вероятностное прогнозирование. Статистическая классификация (метод распознавания образов). Модели неисправностей цифровых устройств. Таблица функций неисправности. Понятие существенного пути. Метод Рота (d-алгоритм). Особенности построения алгоритмов тестирования цифровых устройств TEST-DETECT. **Показатели технического диагностирования.** Показатели технического диагностирования. Особенности. Вероятностный подход к оценке решений при диагностировании технических средств. Ошибки I-го и II-го рода. Процессы накопления отказов и их оценка. Внезапные и постепенные отказы. Оптимизация процессов оценки функционального состояния ЗТКС. Изменение надёжности ЗТКС в процессе функционального состояния. Оценка состояния сложных систем при неравноправных наблюдениях входа и выхода. Влияние проверок на эксплуатационную надёжность ЗТКС. **Методы представления сигналов цифровых ТКС.** Особенности представления цифровых сигналов. Диаграмма как способ иллюстрации цифровых сигналов. “Глазковые” диаграммы. Диаграммы состояний. Алгоритмические диаграммы – диаграмма Треллиса и древовидная диаграмма. **Методология измерения параметров цифровых ТКС.** Двоичный канал и методы оценки его параметров. Возникновение ошибок по битам и их влияние на параметры цифровой передачи. Основные параметры, измеряемые в бинарном канале. Тестовые последовательности. Вычисление параметров ошибок в цифровых каналах. Методология измерений без отключения каналов. Объективизация измеренных результатов. Методы нормирования параметров цифровых каналов. Методологии ITV-T рекомендации G.821, G.826, M.2100. Измерение параметров аналогово-цифровых преобразований НКМ. **Измерения характеристик систем передачи информации.** Методология измерений джиттера в цифровых системах передачи. Необходимость измерений джиттера. Устройство анализатора джиттера. Измерение джиттера составного канала. Измерения, проводимые на ВОЛС. Системное оборудование для анализа волоконных кабелей. Концепция измерений электрических кабелей. Измерение магистральных кабелей. Измерение абонентских кабелей. Измерение структурированных кабельных систем. Особенности радиочастотных измерений. Измерения радиоэфира. Измерения характеристик ретранслятора. Измерение характеристик радиочастотного спектра. Комплексные измерения радиочастотных трактов. **Специальные исследования функционального состояния ЗТКС.** Специальные исследования в области защиты речевой информации. Выявление с использованием контрольно-измерительной аппаратуры возможных технических каналов утечки защищаемой речевой информации от основных и вспомогательных технических средств и систем и оценки соответствия защиты информации требованиям нормативных документов. Специальные исследования в области защиты цифровой информации. Выявление с использованием контрольно-измерительной аппаратуры возможных технических каналов утечки защищаемой цифровой информации.

Рекомендуемый перечень лабораторных работ*:*

1. Исследование параметров, описывающих функциональное состояние ТКС;

2. Прогнозирование функционального состояния ТКС по результатам предварительного контроля;

3. Исследование процессов управления состоянием ТКС в результате диагностирования последних;

4. Исследование полумарковской модели процесса определения функционального состояния ЗТКС;

5. Определение оптимального времени предупредительных замен «стареющих» элементов ЗТКС;

6. Контроль эффективности защиты речевой информации в технических средствах передачи информации с помощью программно-аппаратного комплекса «СПРУТ-МИНИ»;

7. Контроль эффективности защиты информации в средствах вычислительной техники от утечки информации через побочные электромагнитные излучения и наводки с помощью программно-аппаратного комплекса «НАВИГАТОР-ПЗГ»;

8. Исследование полумарковской модели процесса определения функционального состояния ЗТКС.

Рекомендуемый перечень основной литературы:

1. Измерения в телекоммуникационных системах: учебное пособие / А.В. Аминев, А.В. Блохин. – Екатеринбург: Изд-во Урал. ун-та, 2015. – 224 с.

2. Березкин Е.Ф. Надежность и техническая диагностика. – М.: Изд-во Лань, 2019. – 264 с.

3. Техническая диагностика электронных средств: учебник для высшего профессионального образования. / В.Т. Ерёменко и др. – Орел: ФГБОУ ВПО «Госуниверситет - УНПК», 2012. – 157 с.

4. Бычков Е.Д. Основы технической диагностики телекоммуникационных систем: учебное пособие. – Омск, Омский государственный университет путей сообщения, 2020. – 189 с.

5. Хамадулин Э.Ф. Методы и средства измерений в телекоммуникационных системах: учебное пособие для академического бакалавриата. – М.: Издательство Юрайт, 2019. – 365 с.

Перечень материально-технического обеспечения:

программно-аппаратные комплексы «НАВИГАТОР-ПЗГ», «СПРУТ-МИНИ».

**Б.1.С.11.1. Дисциплина «Основы цифровых телекоммуникационных сетей»**

Коды формируемых компетенций: ОПК-11.1.

В результате изучения дисциплины студент должен

знать:

- методы и алгоритмы обеспечения безопасности систем подвижной цифровой защищенной связи;

уметь:

- выбирать методы и разрабатывать алгоритмы обеспечения безопасности систем подвижной цифровой защищенной связи;

владеть:

- базовыми навыками реализации алгоритмов обеспечения безопасности систем подвижной цифровой защищенной связи.

Примерное распределение часов: трудоемкость дисциплины 10 з.е., 360 час.

Форма контроля: 2 экзамена.

Содержание дисциплины:

**Методы множественного доступа к каналу**. Система Т-каналов. Область применения. **Технология PDH**. Международная версия PDH. Методы мультиплексирования в PDH. Способы синхронизации и защиты от ошибок в PDH. Преимущества и недостатки PDH. **Технология SDH**. Отличия SDH от PDH. Методы мультиплексирования в SDH. Способы синхронизации и защиты от ошибок в SDH. Типы оборудования SDH. Топологии и решения. Системы сигнализации в сетях телекоммуникаций. **Технология DWDM**. Принцип работы DWDM. Типовые топологии. **Технологии WAN**. **Технологии LAN**. Технология HDLC. Технология FrameRelay. Контроль работоспособности в FrameRelay. Технология ArcNet. Технология Ethernet. Технология TokenRing. Технология FDDI. Технология ATM. Контроль работоспособности в сетях ATM. Эффективность способов защиты от ошибок в пакетных сетях. **Классификация атак по уровням модели OSI**. Атаки на физическом уровне модели ISO. Атаки на протоколы VLAN. Атаки на протоколы маршрутизации. Атаки на протоколы транспортного уровня. Сканирование сети. Атаки на уровне приложений. **Протоколы защиты Wi-Fi**. Атаки на сети Wi-Fi. Защита устройств беспроводных сетей. **Средства защиты сетевого уровня**. Межсетевые экраны сетевого уровня. Межсетевые экраны уровня приложений. **Организация виртуальных частных сетей**. Варианты построения виртуальных частных сетей. Семейство протоколов IPSec. Ассоциации безопасности и протоколы управления и обмена ключами. **Системы обнаружения вторжений**.

Рекомендуемый перечень основной литературы:

1. Олифер В.Г.; Олифер Н.А. Компьютерные сети. – СПб.: Питер, 2004. –   
864 с.

2. Ротков Л.Ю., Рябов А.А., Виценко А.Ю. Современные сетевые технологии, технологии Интернет: учеб. пособие. – Н. Новгород: ННГУ, 2002. – 244 с.

3. Малышенко Ю.В., Федоров В.В. Защита информации в вычислительных сетях, системах и комплексах: учебное пособие. – М.: РИО РТА, 2007. – 108 с.

**Б.1.С.11.2. Дисциплина «Свойства беспроводных каналов связи»**

Коды формируемых компетенций: ОПК-11.1, ОПК-11.3.

В результате изучения дисциплины студент должен

знать:

- характеристики беспроводных каналов связи и методы их расчета;

- способы разнесенного приема сигналов;

уметь:

- рассчитывать основные характеристики беспроводных каналов связи;

- использовать разнесенный прием сигналов для повышения безопасности систем подвижной цифровой защищенной связи.

Примерное распределение часов: трудоемкость дисциплины 3 з.е., 108 час.

Форма контроля: экзамен.

Содержание дисциплины:

**Передача сигнала в свободном пространстве.** Связь мощностей принятого и передаваемого сигналов. **Многолучевое распространение сигнала.** Квадратичная формула Введенского для множителя ослабления. **Замирания сигнала.** Распределение Релея и Райса. Частотная дисперсия сигнала. Угловая дисперсия сигнала и его пространственная корреляция. **Разнесенный прием.** Выигрыш в системе с разнесенным приемом. **Вероятность битовой ошибки в релеевском и райсовском некоррелированном и коррелированном каналах.** **Оценивание канала в системах связи, использующих OFDM сигналы.**

Рекомендуемый перечень основной литературы:

1. Ермолаев В.Т., Флаксман А.Г. Теоретические основы обработки сигналов в беспроводных системах связи. – Н. Новгород, ННГУ, 2011. – 368 с.

2. Ермолаев В.Т., Мальцев А.А., Флаксман А.Г., Болховская О.В., Клюев А.В. Мобильная связь: вопросы теории и типовые задачи. Учебное пособие. – Н. Новгород: Издательство ННГУ, 2014. – 234 с.

**Б.1.С.11.3. Дисциплина «Беспроводные системы связи и их безопасность»**

Коды формируемых компетенций: ОПК-11.2.

В результате изучения дисциплины студент должен

знать:

- аппаратное и программное обеспечение узлов и устройств систем подвижной цифровой защищенной связи;

- методы контроля работоспособности и оценки эффективности программно-аппаратных средств защиты информации в системах подвижной цифровой защищенной связи;

уметь:

- оценивать эффективность средств защиты информации в системах подвижной цифровой защищенной связи;

владеть:

- навыками контроля работоспособности программно-аппаратных средств защиты информации в системах подвижной цифровой защищенной связи.

Примерное распределение часов: трудоемкость дисциплины 6 з.е., 216 час.

Форма контроля: экзамен.

Содержание дисциплины:

**MAC уровень стандарта IEEE 802.11a**. Независимые зоны обслуживания (ad-hoc сети). Зоны обслуживания с точкой доступа. Понятие скрытого узла. Понятие о механизме «множественного доступа с контролем несущей и предотвращением коллизий». **Физический уровень стандарта IEEE 802.11a**. Основные параметры стандарта. Структура фрейма. Временная и частотная структура субфреймов "PREAMBLE", "SIGNAL" и "DATA". Модуляция данных. **Архитектура и функциональное назначение логических узлов опорной сети и сети радиодоступа**. Синхронизация и поиск соты в LTE. Архитектура и функциональное назначение протоколов Layer 1, Layer 2, Layer 3. Процедура случайного доступа. **Технология множественного доступа OFDMA**. Технология множественного доступа SC-FDMA, отличия SC-FDMA от OFDMA. **Физический уровень стандарта LTE Rel-8/9**. Отличительные особенности и основные процедуры обработки сигналов, передаваемых от абонентов на базовые станции в LTE Rel-8/9. Локализованное и распределённое отображение частотных выборок на поднесущие в SC-FDMA, преимущества и недостатки. Временные структуры кадра LTE. Ресурсная сетка LTE, расстояние между поднесущими, длительность OFDM символа, частота дискретизации, поддерживаемые полосы частот. Функциональное назначение и обработка сигналов в физическом канале PBCH. Опорные (пилотные) сигналы, пример процедуры оценивания канала. Пространственное мультиплексирование Closed-loop в LTE Rel-8/9. Функциональное назначение и обработка сигналов в физических каналах PCFICH и PHICH. Опорные сигналы, используемые при передаче от абонентов на базовые станции в LTE Rel-8/9. Разнесённая передача сигналов от базовой станции абонентам, пространственное мультиплексирование Open-loop в LTE Rel-8/9. Функциональное назначение и обработка сигналов в канале PUCCH. **Физический уровень стандартов Wi-Fi IEEE802.11a/g, WiGig IEEE802.11ad**.

**Б.1.С.11.4. Дисциплина «Системы позиционирования подвижных объектов»**

Коды формируемых компетенций: ОПК-11.3.

В результате изучения дисциплины студент должен

знать:

- принципы построения и функционирования наземных радионавигационных систем дальнего и ближнего действия, обеспечивающих безопасную работу систем подвижной цифровой защищенной связи;

- принципы построения и функционирования спутниковых радионавигационных систем, обеспечивающих безопасную работу систем подвижной цифровой защищенной связи;

уметь:

- реализовывать методы и алгоритмы измерения навигационных параметров, применяемые в радионавигационных системах;

- реализовывать методы и алгоритмы определения местоположения подвижного объекта.

Примерное распределение часов: трудоемкость дисциплины 3 з.е., 108 час.

Форма контроля: зачет.

Содержание дисциплины:

**Общие сведения о системах позиционирования подвижных объектов.** Методы измерения навигационных параметров, применяемые в радионавигационных системах. Методы определения местоположения подвижного объекта. **Принципы построения и функционирования наземных радионавигационных систем дальнего и ближнего действия. Принципы построения и функционирования спутниковых радионавигационных систем.**

Рекомендуемый перечень основной литературы:

1. Авиационная радионавигация: Справочник. А. А. Сосновский, И. А. Хаймович и др. / Под ред. А. А. Сосновского. – М.: Транспорт, 1990.

2. Бакулев П. А., Сосновский А. А. Радионавигационные системы. Учебник для вузов. – М.: Радиотехника, 2005.

3. ГЛОНАСС. Принципы построения и функционирования. / Под ред. А.И. Пе­рова, В.Н. Харисова*.* Изд. 4-е, перераб. и доп. – М.: Радиотехника, 2010.

4. Яценков В.С. Основы спутниковой навигации. Системы GPS NAVSTAR и ГЛОНАСС. – М: Горячая линия-Телеком, 2005.

5. Баженов А.В. Радионавигационные системы. Учебное пособие. – Ставрополь: СВВАИУ(ВИ), 2007.

6. Беляевский Л.С., Новиков В.С., Олянюк П.В. Основы радионавигации: Учебник для вузов гражд. авиации. – М.: Транспорт, 1982.

**Б.1.С.11.5. Дисциплина «Алгоритмы идентификации динамических моделей криптосистем»**

Коды формируемых компетенций: ОПК-11.2.

В результате изучения дисциплины студент должен

знать:

- основные подходы к построению математических моделей криптосистем и их функциональных элементов как динамических объектов;

уметь:

- определять базовые параметры математических моделей криптосистем;

- оценивать параметры криптографической стойкости шифров на основе базовых параметров их экспериментальных данных.

Примерное распределение часов: трудоемкость дисциплины 5 з.е., 180 час.

Форма контроля: экзамен.

Содержание дисциплины:

**Общая структурная схема криптосистемы.** Динамическая математическая модель в форме синхронного автомата Хаффмана-Глушкова для основных функциональных элементов криптосистемы. **Задача структурной и параметрической идентификации математической модели криптосистемы как задача определения наборов базовых параметров и свободных параметров**. Текстовые последовательности криптосистемы как сигналы, порождаемые гипотетическими источниками экспериментальных данных. Глубина памяти и условие непротиворечивости таблицы истинности прогнозирующего оператора источника экспериментальных данных. Векторные сигналы криптосистемы и объемы их фазовых пространств. Алгоритмическая реализация обработки векторных отсчетов текстовых сигналов. **Основные классы алгоритмов структурной идентификации источников экспериментальных данных**. Оценки вычислительной сложности алгоритмов структурной идентификации относительно длины обрабатываемой последовательности данных. **Основные классы алгоритмов параметрической идентификации источников экспериментальных данных**. Алгоритмы параметрической идентификации линейных математических моделей источников экспериментальных данных. Подходы к построению алгоритмов параметрической идентификации нелинейных математических моделей криптосистем по экспериментальным данным.

Рекомендуемый перечень основной литературы:

1. Васильева И.Н. Криптографические методы защиты информации. – М.: Издательство Юрайт, 2018. – 349 с.

2. Лось А.Б., Нестеренко А.Ю., Рожков М.И. Криптографические методы защиты информации. – М.: Издательство Юрайт, 2018. – 473 с.

3. Кирьянов К.Г. Генетический код и тексты: динамические и информационные модели сложных систем. / Ред. Л.Ю. Ротков, А.В. Якимов. – Нижний Новгород: ТАЛАМ, 2002. – 100 с.

4. Гроп Д. Методы идентификации систем. – М.: Мир, 1979. – 302 с.

5. Эйкхофф П. Современные методы идентификации систем. – М.: Мир, 1983. – 400 с.

**Б.1.С.12.1. Дисциплина «Защита информации от утечки по техническим каналам. Дополнительные главы»**

Коды формируемых компетенций: ОПК-12.1, ОПК-12.2, ОПК-12.3.

В результате изучения дисциплины студент должен

знать:

- технические каналы утечки информации, обрабатываемой средствами вычислительной техники, возможности специальных технических средств по перехвату информации, обрабатываемой средствами вычислительной техники;

- технические каналы утечки акустической речевой информации, возможности средств акустической речевой разведки по перехвату разговоров из выделенных помещений;

- принципы построения и основные характеристики средств защиты объектов информатизации от утечки информации по техническим каналам;

- принципы построения и основные характеристики средств защиты выделенных помещений от утечки речевой информации по техническим каналам;

- организацию защиты объектов информатизации от утечки информации по техническим каналам;

умеет:

- проводить анализ потенциальных технических каналов утечки информации на объектах информатизации и речевой информации в выделенных помещениях;

- обосновывать требования к подсистеме защиты объекта информатизации от утечки информации по техническим каналам.

Примерное распределение часов: трудоемкость дисциплины 7 з.е., 252 час.

Форма контроля: экзамен.

Содержание дисциплины:

**Цели и задачи защиты информации от утечки информации по техническим каналам.** Термины и определения в области защиты информации от утечки по техническим каналам: объект информатизации, выделенное помещение, ОТСС, ВТСС, посторонние проводники, контролируемая зона, утечка по техническому каналу, перехват информации, средство разведки, специальное техническое средство негласного получения информации, технический канал утечки информации. Цели и задачи защиты информации от утечки информации по техническим каналам. Содержание и порядок изучения дисциплины. **Технические каналы утечки информации, обрабатываемой СВТ Электромагнитные и электрические технические каналы утечки информации, обрабатываемой средствами вычислительной техники (СВТ)** Классификация технических каналов утечки информации, обрабатываемой СВТ. Причины возникновения побочных электромагнитных излучений (ПЭМИ) СВТ. Опасная зона R2. Схема технического канала утечки информации, возникающего за счет ПЭМИ СВТ. Причины возникновения электрических технических каналов утечки информации, обрабатываемой СВТ. Случайные антенны. Причины возникновения наводок информативных сигналов в случайных антеннах. Опасная зона r1. Схема технического канала утечки информации, возникающего за счет наводок ПЭМИ СВТ в случайных антеннах. Причины возникновения наводок информативных сигналов в линиях электропитания и цепях заземления СВТ. Схемы технических каналов утечки информации, возникающих за счет наводок ПЭМИ СВТ в линиях электропитания и цепях заземления СВТ. Средства разведки ПЭМИН **Специально создаваемые технические каналы утечки информации, обрабатываемой СВТ** Схема технического канала утечки информации, создаваемого методом «высокочастотного облучения». Средства перехвата информации путем «высокочастотного облучения» СВТ. Схема технического канала утечки информации, создаваемого путем внедрения в СВТ электронных устройств перехвата информации. Электронные устройства перехвата информации, внедряемых в СВТ. **Технические каналы утечки акустической речевой информации Характеристики речи. Классификация технических каналов утечки акустической речевой информации.** Акустические сигналы. Линейные и энергетические характеристики акустического поля. Характеристики речи (семантические, фонетические, физические). Спектр и типовые уровни речевого сигнала. Разборчивость речи. Методы оценки разборчивости речи. **Прямые акустические каналы утечки речевой информации**. Способы перехвата речевой информации из выделенных помещений по прямому акустическому каналу. Схемы перехвата информации по прямым акустическим каналам утечки информации. Средства акустической разведки с датчиками микрофонного типа: цифровые диктофоны, электронные устройства перехвата речевой информации, направленные микрофоны. **Акустовибрационные и акустооптический каналы утечки речевой информации.** Способы перехвата речевой информации из выделенных помещений по акустовибрационным каналам. Схемы перехвата речевой информации по акустовибрационным каналам. Электронные стетоскопы. Радиостетоскопы. Способы перехвата речевой информации из выделенных помещений по акустооптическому каналу. Схема перехвата речевой информации по акустооптическому каналу. Лазерные акустические системы разведки. **Акустоэлектрические и акустоэлектромагнитные каналы утечки речевой информации.** Причины возникновения акустоэлектрические каналов утечки речевой информации. Акустоэлектрические преобразователи генераторного типа. Акустоэлектрические преобразователи модуляторного типа. Способы перехвата речевой информации из выделенных помещений по акустоэлектрическим каналам. Схема пассивного акустоэлектрического канала утечки речевой информации. Схема активного акустоэлектрического канала утечки речевой информации. Причины возникновения акустоэлектромагнитных каналов утечки речевой информации. Способы перехвата речевой информации из выделенных помещений по акустоэлектрическим каналам. Схема пассивного акустоэлектромагнитного канала утечки речевой информации. Схема активного акустоэлектромагнитного канала утечки речевой информации. **Технологии защиты объектов информатизации от утечки информации по техническим каналам. Экранирование и заземление технических средств.** Классификация способов и средств защиты объектов информатизации от утечки информации по техническим каналам. Экранирование технических средств их соединительных линий. Экранирующие материалы. Экранированные помещения (экранированные камеры). Защищенные ПЭВМ. Заземление технических средств. Требования к заземлению ОТСС. Схемы заземления ОТСС. Методы и средства измерения сопротивления заземления ОТСС. **Системы пространственного электромагнитного зашумления** Требования к системе пространственного электромагнитного зашумления. Принципы построения систем пространственного электромагнитного зашумления и широкополосных генераторов шума. Основные характеристики сертифицированных систем пространственного электромагнитного зашумления (САЗ типа А). Требования по установке систем пространственного электромагнитного. Особенности зашумления инженерных коммуникаций. **Способы и средства защиты объектов информатизации от утечки информации по цепям электропитания и заземления** Требования к системе электропитания ОТСС. Требования к помехоподавляющим фильтрам, используемым для защиты цепей электропитания СВТ. Принципы построения, основные характеристики и требования по установке сертифицированных помехоподавляющих фильтров. Принципы построения систем линейного электромагнитного зашумления и их основные характеристики (САЗ типа Б). Требования по установке систем линейного электромагнитного зашумления. **Технологии защиты выделенных помещений от утечки речевой информации по техническим каналам Классификация способов и средств защиты выделенных помещений от утечки речевой информации по техническим каналам** Пассивные способы защиты выделенных помещений от утечки речевой информации по техническим каналам. Активные способы защиты выделенных помещений от утечки речевой информации по техническим каналам. Звуко- и виброизоляция выделенных помещений, глушители шума. Звукопоглощающие материалы. Специальные защищенные помещения. **Системы и средства виброакустической маскировки** Требования к системе виброакустической маскировки. Принципы построения низкочастотных генераторов шума. Принципы построения акустических излучателей и виброизлучателей. Основные характеристики сертифицированных систем виброакустической маскировки типа А. Основные характеристики сертифицированных систем виброакустической маскировки типа Б. Особенности установки акустических излучателей и виброизлучателей в выделенных помещениях. Специальная аппаратура для ведения конфиденциальных переговоров. **Средства защиты ВТСС от утечки речевой информации по акустоэлектрическим каналам** Пассивные способы защиты ВТСС от утечки речевой информации по акустоэлектрическим каналам (ограничение сигналов малой амплитуды, фильтрация высокочастотных сигналов навязывания, отключение акустоэлектрических преобразователей опасных сигналов). Активные способы защиты ВТСС от утечки речевой информации по акустоэлектрическим каналам. Принципы построения и основные характеристики средств защиты ВТСС, основанных на использовании ограничителей малой амплитуды и фильтров нижних частот. Принципы построения основные характеристики средств защиты ВТСС, основанных на отключении акустоэлектрических преобразователей. Принципы построения основные характеристики средств защиты ВТСС, основанных на использовании низкочастотных генераторов шума. **Специальные технические средства подавления электронных устройств перехвата речевой информации** Принципы построения и основные характеристики подавителей диктофонов. Принципы построения и основные характеристики широкополосных генераторы шума. Принципы построения и основные характеристики блокираторов средств сотовой связи. Организация защиты информации от утечки по техническим каналам на объектах информатизации **Порядок организации защиты информации от утечки по техническим каналам.** Предпроектное специальное обследование объекта информатизации. Обоснование требований к подсистемезащиты информации от утечки по техническим каналам (СЗИУТК). Содержание технического задания на создание (СЗИУТК). **Разработка технические решений по защите объекта информатизации от утечки.**

Рекомендуемый перечень лабораторных работ:

1. Исследование спектров сигналов.

2. Исследование основных характеристик случайных приемных антенн.

3. Исследование побочных электромагнитных излучений (ПЭМИ) ПЭВМ.

4. Исследование ПЭМИ ПЭВМ.

5. Оценка возможностей по перехвату ПЭМИН СВТ.

6. Исследование акустических и акустовибрационых каналов утечки речевой информации.

7. Оценка возможностей по перехвату речевой информации из выделенного помещения средствами акустической разведки.

8. Исследование подверженности ВТСС акустоэлектрическим преобразованиям.

9. Исследование основных характеристик систем пространственного и линейного электромагнитного зашумления.

10. Исследование характеристик помехоподавляющих фильтров типа «ФП»

11. Исследование характеристик системы виброакустической защиты типа Б.

12. Исследование характеристик средств защиты ВТСС от утечки информации по техническим каналам.

13. Исследование характеристик специальных средств радиоподавления.

14. Предпроектное специальное обследование объекта информатизации.

15. Обоснование требований к подсистеме защиты объекта информатизации от утечки информации по техническим каналам (СЗИУТК).

16. Разработка технических решений по защите объекта информатизации от утечки информации по техническим каналам.

Рекомендуемый перечень основной литературы:

1. Технические средства и методы защиты информации: учебник. / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков. – 7-е изд., испр. и доп. – М.: Горячая линия-Телеком, 2018. – 444 с.

2. Хорев А.А. Техническая защита информации: учебное пособие: В 3-х т. Т. 1: Технические каналы утечки информации. – М.: НПЦ «Аналитика», 2008. –   
436 с.

Перечень материально-технического обеспечения:

лаборатория технической защиты информации, оснащенная специализированным оборудованием по защите информации от утечки   
по акустическому, акустоэлектрическому каналам, каналу побочных электромагнитных излучений и наводок, техническими средствами контроля эффективности защиты информации от утечки по указанным каналам.

**Б.1.С.12.2. Дисциплина «Программно-аппаратные средства защиты информации. Дополнительные главы»**

Коды формируемых компетенций: ОПК-12.1, ОПК-12.2, ОПК-12.3.

В результате изучения дисциплины студент должен

знать:

- основные классы и виды уязвимостей программного обеспечения, угрозы несанкционированного доступа к информации и специальных программных воздействий на информацию и ее носители в автоматизированных системах;

- способы и средства защиты информации, обрабатываемой автоматизированными системами, от несанкционированного доступа и специальных программных воздействий на нее;

- методы и средства контроля защищенности информации, обрабатываемой автоматизированными системами, от несанкционированного доступа и специальных программных воздействий на нее;

уметь:

- применять технологии защиты информации от несанкционированного доступа для обеспечения безопасности автоматизированных систем и вычислительных сетей;

- проводить контроль защищенности информации, обрабатываемой автоматизированными системами, от несанкционированного доступа.

Примерное распределение часов: трудоемкость дисциплины 8 з.е., 288 час.

Форма контроля: экзамен.

Содержание дисциплины:

Угрозы и уязвимости информации при обработке в автоматизированных системах (АС). Понятие технологий обеспечения безопасности. Модели угроз безопасности информации, обрабатываемой и источники уязвимостей АС и их характеристика. Классификация способов обеспечения информационной безопасности (управление доступом; регистрация и учет; обеспечение целостности; контроль отсутствия недекларированных возможностей; антивирусная защита; криптографическая защита информации; межсетевое экранирование и сегментирование сетей; анализ защищенности и обнаружение вторжений; предотвращение утечек и т.д.). Основные функциональные задачи информационной безопасности и их реализация для сетевой безопасности модель ААА (аутентификация, авторизация и акаунтинг). Задачи и основные принципы сетевой безопасности Проблемы обеспечения информационной безопасности в распределенных вычислительных сетях. Важность, актуальность и сложность решения задач обеспечения сетевой безопасности. Интеграция принципов защиты вычислительных систем и сетей передачи данных. Основные функциональные задачи информационной безопасности и их реализация для сетевой безопасности модель ААА (аутентификация, авторизация и акаунтинг) в сетях. Уровни стека протоколов TCP/IP. Соотношение с моделью ISO-OSI. Возможные угрозы сети на различных уровнях стека протоколов. Структура сетевых атак. Банк данных о атаках и уязвимостях. Матрица MITRE. Технологии идентификации и аутентификации Аутентификация, авторизация и идентификация (определения). Технологии аутентификации: одноразовые пароли, многоразовые пароли, базы учетных записей, многофакторная аутентификация. Технологии идентификации и аутентификации пользователей по специальным устройствам. Технологии идентификации и аутентификации пользователей по биометрическим характеристикам человека. Технологии идентификации и аутентификации используемых компонентов обработки информации (аппаратных и программных средств) Технологии аутентификации на основе симметричных криптосистем Аутентификация на основе симметричных криптографических протоколов. Протоколы взаимной аутентификацию Протоколы с распределением колючей. Двух, трех и многосторонние протоколы. Виды атак на протоколы аутентификации. Протоколы ISO. Протокол Нидхема-Шрейдера. Другие виды протоколов. Технологии аутентификации на основе асимметричных криптосистем Аутентификация на основе ключевых хеш-функций. Аутентификация на основе асимметричных критографических протоколов. Модификация парольной схемы. Использование цифровой подписи. Структуры PKI. Протоколы взаимной аутентификациию Протоколы с распределением колючей. Двух, трех и многосторонние протоколы. Виды атак на протоколы аутентификации. Протоколы ISO. Протокол Нидхема-Шрейдера. Другие виды протоколов. Технологии аутентификации на основе хеш-функций Особенности использования хеш-функций. Технологии построения ключевых хеш-функций на осонове бесключевых. Протоколы аутентификации. Аутентификация в сетях WiFi, GSM, GPRS, LTE. Протоколы аутентификации и авторизации в вычислительных сетях Простейшие протоколы удаленной аутентификации: PAP и CHAP. Аутентификация и авторизация. Сетевые протоколы и службы авторизации: RADIUS, TACACS, KERBEROS. Аутентификация в беспроводных сетях. Современные технологии управления доступом к информации, модель механизма защиты: Субъектно-объектная модель управления доступом. Модель абстрактного механизма защиты и политики безопасности. Современные технологии управления доступом к информации, использующие дискреционный принцип: Технологии управления доступом к АРМ и серверам. Технологии управления учетными записями. Дискреционный принцип доступа. Модели Грехема-Денинига, Хартсона, HRU, T-G. Реализации этих моделей в информационных системах. Сравнение результатов моделирования. Задачи по анализу передачи прав или утечки информации. Современные технологии управления доступом к информации, использующие мандатный принцип: Принципы военной безопасности MLS. Понятие решетки безопасности. Модель Деннинг. Технологии управления доступом на основе мандатного принципа. Модели Белла-ЛаПадулы (простая, RW, классическая и пр.). Реализации этих моделей в информационных системах. Современные технологии управления доступом к информации, использующие тематический принцип: Принципы тематического подхода. Примеры и типы тематических моделей. Построение тематических решеток безопасности. Монорубрицированные классификации. Мультирубрицированные классификации. Реализации тематических моделей в информационных системах. Современные технологии управления доступом к информации, использующие ролевой принцип: Принципы ролевого подхода. Примеры и типы ролевых моделей. Индивидуально-групповое управление доступом. Реализации ролевых моделей в информационных системах. Современные технологии управления доступом для обеспечения целостности информации: Основные требования к подсистеме обеспечения целостности информации. Подсистема резервного копирования: основные требования к подсистеме резервного копирования; типы резервного копирования; типы резервных носителей; хранение и использование резервных копий; архитектура подсистемы резервного копирования. Подсистема распределения обновлений: основные требования к подсистеме распределения обновлений; возможные варианты построения системы; архитектура подсистемы распределения обновлений. Модель Биба. Современные технологии контроля доступа в вычислительных сетях Задачи фильтрации сетевого трафика. Межсетевые экраны. Фильтрация пакетов. Коммутация каналов. Анализ приложений. Анализ состояний. Прокси сервер. Понятие DMZ. Современные технологии обеспечения изоляции, изоляция в сети, защищенные сетевые протоколы. Основные требования к обеспечению изоляции. Изоляция в операционных системах, в СУБД, в сетях. Реализации технологии изоляции. Развитие IPv4 и свойства защищенности протокола IPv6. Протоколы IPsec, SSL, TLS, PPTP. Построение VPN Пассивные сетевые атаки. Атаки не нарушающие функционирование сети. Сбор информации выбор целей, подготовка проникновения. Анонимное сканирование. Возможности обнаружения пассивных атак. Активные сетевые атаки. Атаки на слабости протоколов. Имперсонация. Методы внедрения ложного сервера. MitM атаки. Методы десинхронизации TCP соединений. DOS атаки. Системы выявления утечек и обнаружения вторжений. Задачи сетевого мониторинга на разных уровнях стека протокола TCP\IP. DLO, IDS и IPS системы. Современные технологии обеспечения безопасности информации в виртуальных машинах и сетях, в Центрах Обработки Данных и при выполнении «облачных вычислений»: Назначение Центра Обработки Данных (ЦОД) и виртуальных сред. Характерные особенности виртуализации с точки зрения ИБ. Угрозы безопасности виртуальным инфраструктурам. Основные требования по обеспечению ИБ виртуальных инфраструктур. Обеспечение ИБ при переходе к «облачным» вычислениям. Скрытые каналы утечки информации. Утечки информации в статистических БД. Понятие примеры и классификация скрытых каналов. Методы и средства борьбы со скрытыми каналами. Общие вероятностные модели – невлияния и невыводимоти. Автоматная модель невмешательства. Анонимные сети. Понятие анонимных сетей. Примеры анонимных сетей. TOR. I2P. Уязвимости. Обнаружение. Специальные сети и глобальные сети. Альтернативные топологии. Проблема маршрутизации. Атаки на интернет. «Требования по защите автоматизированных систем от несанкционированного доступа к информации» Системы защиты информации от несанкционированного доступа (НСД) в автоматизированной системе (АС) на базе автономного автоматизированного рабочего места (АРМ). Состав системы защиты информации от НСД в АС на базе автономного АРМ. Показатели защищенности СВТ от несанкционированного доступа к информации. Требования к показателям защищенности СВТ различных классов. Классификация АС. Требования по защите информации от НСД для АС различных классов. Системы защиты информации от несанкционированного доступа в локальных и корпоративных сетях. Состав системы защиты информации от несанкционированного доступа в локальных и корпоративных сетях. Классификация межсетевых экранов (МЭ). Требования к различным классам защищенности МЭ. Системы обнаружения и предупреждения сетевых вторжений. Основные требования по защите автоматизированных систем от несанкционированного доступа к информации Основные требования по защите автоматизированных систем обработки информации, составляющей государственную тайну. Основные требования по защите информационных систем персональных данных. Основные требования по защите государственных информационных систем общего пользования. Критерии оценки безопасности информационных технологий (ГОСТ 15408). Основные положения и понятия «Общих критериев», функции безопасности, профиль защиты, функции доверия, оценочные уровни, верификация выполнения требований. Требования к составу и содержанию функций защиты информации для конкретных сервисов безопасности: антивирусных средств, средств доверенной загрузки и средств предупреждения сетевых вторжений. «Системы и средства защиты информации от несанкционированного доступа» Программные средства защиты в составе операционных систем и систем управления базами данных. Типовой состав и назначение средств защиты ОС и СУБД, установка и управление их функционированием (настройка). Антивирусные программы. Сертифицированные средства антивирусной защиты. Средства антивирусной защиты иностранного производства. Программно-аппаратные средства аутентификации и доверенной загрузки. Типы программно-аппаратных средств аутентификации. Обзор современных средств аутентификации. Типы средств доверенной загрузки. Обзор современных программно-аппаратных средств доверенной загрузки. Программные и программно-аппаратные средства защиты информации от несанкционированного доступа в АС на базе автономного АРМ. Типовой состав и назначение средств защиты информации от НСД. Обзор современных программно-аппаратных средств защиты информации от НСД в АС на базе автономного АРМ. Программные и программно-аппаратные средства сетевой безопасности. Программные и программно-аппаратные межсетевые экраны. Программные и программно-аппаратные средства обнаружения вторжений. Средства создания виртуальных защищенных сетей. «VipNet». С-Терра VPN. Средства контроля защищенности информации от несанкционированного доступа. Средство фиксации и контроля исходного состояния программного комплекса «ФИКС». Средство создания модели системы разграничения доступа «Ревизор 1 ХР». Средство контроля защищенности от несанкционированного доступа «Ревизор 2 ХР». Программа поиска и гарантированного уничтожения информации на дисках TERRIER. Сканеры безопасности. Сканер безопасности «Сканер-ВС». Сканер безопасности «Ревизор сети». Сканер безопасности XSpaider.

Рекомендуемый перечень лабораторных работ:

1. Технологии обеспечения безопасности операционных систем Linux.

2. Технологии обеспечения безопасности операционных систем Windows.

3. Реализации матрицы доступа и проверка введенных ограничений по доступу в операционной системе.

4. Исследование возможностей расширения технологий защиты от несанкционированного доступа к информации с использованием мандатной и ролевой моделей доступа в SELinux.

5. Исследование сетевых атак.

6. Обоснование требований к системе защиты распределенной автоматизированной системы на основе ОС Windows Server от несанкционированного доступа к информации.

7. Обоснование требований к системе защиты вычислительной сети от активных атак и сетевых вторжений.

8. Разработки технических решений по защите вычислительной сети на основе систем обнаружения и предупреждения вторжений (IDS/IPS), их развертывание в сети и настройка.

9. Технологии восстановления системного и прикладного программного обеспечения после сбоев и отказов оборудования и программно-математического воздействия средствами операционных систем Windows.

10. Технологии проверки целостности данных и резервирование: надежность данных в операционных систем Linux.

11. Создание защищенных каналов с помощью OpenVPN.

12. Скрытый канал для передачи данных ICMP Tunnel.

13. Установка и настройка программных средств защиты АС на базе АРМ (ОС Windows (7, 8), «Фикс»).

14. Установка и настройка средств антивирусной защиты.

15. Установка и настройка программного комплекса защиты АС на базе АРМ от несанкционированного доступа к информации «Панцирь».

16. Установка и настройка программного комплекса для организации защищенных виртуальных сетей и распределенного межсетевого экранирования «Застава».

17. Установка и настройка программно-аппаратного комплекса для обеспечения сетевой безопасности корпоративной сети С-Терра CSP VPN.

18. Контроль защищенности АС на соответствие требованиям по защите информации от несанкционированного доступа с использованием средств контроля защищенности «Ревизор 1», «Ревизор 2», «TERRIER», «ФИКС».

19. Контроль защищенности АС на соответствие требованиям по защите информации от несанкционированного доступа с использованием сканеров безопасности «Сканер-ВС», «Ревизор сети», «Xspider».

Рекомендуемый перечень основной литературы:

1. Мельников Д.А. Информационная безопасность открытых систем: учебник. – М.: Флинта: Наука, 2014. – 448 с.

2. Программно-аппаратные средства защиты информации: учебное пособие. / В.А. Воеводин, А.В. Душкин, А.Н. Петухов, А.А. Хорев; под ред. А.А. Хорева. – М.: МИЭТ, 2021. – 280 с.

3. Программно-аппаратные средства защиты информации: учебно-методическое пособие. / А.В. Душкин, О.Р. Лукманова, А.Н. Петухов, А.А. Хорев; под ред. А.А. Хорева. – М.: МИЭТ, 2021. – 216 с.

4. Управление безопасностью критических информационных инфраструктур: учебное пособие / А.Н. Петухов, П.Л. Пилюгин, А.В. Душкин, Ю.А. Губсков; под ред. А.В. Душкина. – М.: МИЭТ, 2021. – 208 с.

Перечень материально-технического обеспечения:

лаборатория программно-аппаратных средств защиты информации.

**Б.1.С.12.3. Дисциплина «Аттестация объектов информатизации»**

Коды формируемых компетенций: ОПК-12.1, ОПК-12.2, ОПК-12.3.

В результате изучения дисциплины студент должен

знать:

- нормативные правовые акты, методические документы, национальные стандарты в области аттестации объектов информатизации;

- методы, средства и методики контроля защищенности информации от утечки по техническим каналам;

- порядок проведения аттестации объектов информатизации на соответствие требованиям по защите информации;

- отчетные документы, оформляемые по результатам аттестации объектов вычислительной техники на соответствие требованиям по защите информации;

уметь:

- разрабатывать программы и методики аттестационных испытаний объектов вычислительной техники на соответствие требованиям по защите информации;

- проводить аттестационные испытания объектов вычислительной техники на соответствие требованиям по защите информации;

- оформлять материалы аттестационных испытаний (протоколы аттестационных испытаний и заключения по результатам аттестации объектов вычислительной техники на соответствие требованиям по защите информации);

- оформлять аттестат соответствия объектов вычислительной техники требованиям по защите информации.

Примерное распределение часов: трудоемкость дисциплины 5 з.е., 180 час.

Форма контроля: экзамен.

Содержание дисциплины:

Методы и средства контроля эффективности защиты информации, обрабатываемой СВТ. Методы и средства контроля эффективности защиты информации, обрабатываемой СВТ: Показатели эффективности защиты информации, обрабатываемой СВТ, от утечки по техническим каналам. Методы контроля эффективности защиты информации, обрабатываемой СВТ. Требования к средствам измерения ПЭМИН СВТ и условиям проведения измерений. Порядок проведения контроля эффективности защиты СВТ от утечки информации, возникающей за счет ПЭМИН: Порядок проведения аттестационных испытаний СВТ при контроли эффективности защиты СВТ от утечки информации, возникающей за счет ПЭМИ. Порядок проведения аттестационных испытаний СВТ при контроле эффективности защиты СВТ от утечки информации, возникающей за счет наводок информативных сигналов на токопроводящие коммуникации. Методы и средства контроля эффективности защиты речевой информации. Методы и средства контроля выполнения норм защищенности речевой информации от утечки по техническим каналам: Показатели защищенности речевой информации от утечки речевой информации по техническим каналам. Методы контроля эффективности защиты ВП от утечки речевой информации по техническим каналам. Требования к средствам измерения при контроле выполнения норм защищенности речевой информации от утечки по прямым акустическим, акустовибрационным и акустооптическому каналам. Требования к средствам измерения при контроле выполнения норм защищенности речевой информации от утечки по акустоэлектрическим каналам. Порядок проведения контроля выполнения норм защищенности речевой информации от утечки по техническим каналам: Порядок проведения контроля выполнения норм защищенности речевой информации от утечки по прямым акустическим каналам. Порядок проведения контроля выполнения норм защищенности речевой информации от утечки по акустовибрационным и акустооптическому каналам. Порядок проведения контроля вспомогательных технических средств (ВТСС) на подверженность акустоэлектрическим преобразованиям. Порядок проведения контроля ВТСС на подверженность «высокочастотному навязыванию». Методы и средства выявления электронных устройств перехвата речевой информации. Классификация методов поиска электронных устройств перехвата информации: Демаскирующие признаки электронных устройств перехвата информации. Классификация методов и средств поиска электронных устройств перехвата информации. Порядок специальной проверки ВП на наличие возможно внедренных закладочных устройств. Методы и средства поиска электронных устройств перехвата информации: Методы и средства выявления скрытых систем видеонаблюдения. Методы выявления закладочных устройств с использованием ИЭМП. Методы выявления закладочных устройств с использованием нелинейных локаторов и рентгено-телевизионных комплексов. Методы выявления закладочных устройств с использованием сканирующих приемников: Методы выявления закладочных устройств с использованием сканирующих приемников и интерсепторов. Сканирующие приемники (основные характеристики). Интерсепторы. Методы выявления закладочных устройств с использованием программно-аппаратных комплексов: Методы выявления закладочных устройств с использованием ПАКРК. Программно-аппаратные комплексы радиоконтроля (основные характеристики). Методы и средства выявления закладочных устройств, подключаемым к проводным коммуникациям. Программно-аппаратные комплексы анализа проводных коммуникаций (основные характеристики). Организация аттестации объектов информатизации по требованиям безопасности информации. Организация аттестации объектов информатизации: Порядок организации аттестации ОИ (ВП) требованиям по безопасности информации. Подготовка к проведению аттестации ОИ (ВП). Программа и методика аттестационных испытаний ОИ (ВП) Порядок проведения аттестационных испытаний: Порядок проведения аттестационных испытаний ОИ. Порядок проведения аттестационных испытаний ВП Специальное обследование ОИ (ВП) Специальное обследование ОИ. Специальное обследование ВП. Оформление результатов аттестационных испытаний: Протоколы оценки защищенности ОИ (ВП). Заключение по результатам аттестации ОИ (ВП). Аттестат соответствия ОИ (ВП).

Рекомендуемый перечень лабораторных работ:

1. Контроль выполнения норм защищенности СВТ от утечки информации по каналам ПЭМИН.

2. Контроль выполнения норм защищенности СВТ от утечки информации по каналам ПЭМИН.

3. Оценка выполнения норм защищенности СВТ от утечки информации по каналам ПЭМИН.

4. Контроль выполнения норм защищенности речевой информации от утечки по прямым акустическим и акустовибрационным каналам.

5. Оценка выполнения норм защищенности речевой информации от утечки по прямым акустическим, акустовибрационным и акустооптическому каналам.

6. Составление протокола оценки эффективности защиты акустической речевой информации от утечки информации по техническим каналам.

7. Контроль выполнения норм защищенности речевой информации от утечки по акустоэлектрическим и акустоэлектромагнитным каналам:

8. Контроль ВТСС на подверженность акустоэлектрическим преобразованиям.

9. Контроль ВТСС на подверженность акустоэлектромагнитным преобразованиям.

10. Контроль ВТСС на подверженность «высокочастотному навязыванию»

11. Составление протокола оценки эффективности защиты акустической речевой информации от утечки информации по техническим каналам.

12. Выявление закладных устройств с использованием средств поиска индикаторного типа.

13. Поиск закладных устройств с использованием нелинейных локаторов.

14. Поиск закладных устройств с использованием сканирующих радиоприемников и интерсепторов.

15. Выявление закладных устройств с использованием программно-аппаратных комплексов

16. Разработка программы и методики аттестационных испытаний объекта информатизации на соответствие требованиям по безопасности информации.

17. Оформление результатов аттестационных испытаний

18. Разработка протокола оценки защищенности СВТ от утечки информации по каналам ПЭМИН.

19. Разработка протокола оценки выполнения норм противодействия акустической речевой разведке в ВП

20. Разработка заключения по результатам аттестации ОИ (ВП).

Рекомендуемый перечень основной литературы:

1. Технические средства и методы защиты информации: учебник. / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков. – 7-е изд., испр. и доп. – М.: Горячая линия-Телеком, 2018. – 444 с.

2. Хорев А.А. Техническая защита информации: учебное пособие: В 3-х т. Т. 1: Технические каналы утечки информации. – М.: НПЦ «Аналитика», 2008. –   
436 с.

Перечень материально-технического обеспечения:

лаборатория технической защиты информации, оснащенная специализированным оборудованием по защите информации от утечки   
по акустическому, акустоэлектрическому каналам, каналу побочных электромагнитных излучений и наводок, техническими средствами контроля эффективности защиты информации от утечки по указанным каналам.

**Б.1.С.12.4. Дисциплина «Проектирование систем защиты объектов информатизации»**

Коды формируемых компетенций: ОПК-12.1, ОПК-12.2.

В результате изучения дисциплины студент должен

знать:

- нормативные правовые акты, методические документы, национальные стандарты в области проектирования систем защиты информации объектов информатизации;

- нормативные правовые акты, методические документы, национальные стандарты в области проектирования средств и систем информатизации в защищенном исполнении

- порядок создания автоматизированных систем в защищенном исполнении;

- виды испытаний технических средств обработки информации в защищенном исполнении и общие требования к их проведению;

уметь:

- проводить анализ угроз безопасности информации на объекте информатизации;

- проводить предпроектное обследование объекта информатизации;

- разрабатывать аналитическое обоснование необходимости создания системы защиты информации объекта информатизации;

- разрабатывать техническое задание на создание системы защиты информации объекта информатизации;

- разрабатывать техническое задание на создание средства и/или системы информатизации в защищенном исполнении;

- разрабатывать технический проект системы защиты информации объекта информатизации;

- разрабатывать технический проект средства и/или системы информатизации в защищенном исполнении;

- формировать требования к средствам и системам информатизации в защищенном исполнении;

- разрабатывать концепцию средств и систем информатизации в защищенном исполнении;

- разрабатывать программы и методики испытаний средства и/или системы информатизации в защищенном исполнении;

- разрабатывать эксплуатационную документацию на системы защиты информации, организационно-распорядительную документацию по защите информации на объекте информатизации;

- разрабатывать рабочую и эксплуатационную документацию на средства и системы информатизации в защищенном исполнении.

Примерное распределение часов: трудоемкость дисциплины 5 з.е., 180 час.

Форма контроля: экзамен.

Содержание дисциплины:

**Проектирование систем защиты объектов информатизации. Порядок создания системы защиты информации объекта информатизации.** Состав системы защиты информации (СЗИ) объекта информатизации (ОИ). Основные требования к СЗИ ОИ. Стадии и этапы создания СЗИОИ. **Аналитическое обоснование необходимости создания СЗИ ОИ.** Порядок проведения аналитического обоснования необходимости создания СЗИ ОИ. Анализ данных о назначении, функциях, условиях функционирования основных технических средств и систем, установленных на ОИ, и характере обрабатываемой на них информации. Разработка перечня информации (сведений) ограниченного доступа, подлежащих защите на ОИ. Предпроектное обследование ОИ. Классификация АС. Категорирование ОИ. **Модель угроз безопасности информации, обрабатываемой на ОИ.** Методика оценки угроз безопасности информации. Модель угроз несанкционированного доступа к информации, обрабатываемой АС. Модель нарушителя. Модель угроз утечки информации по техническим каналам. **Техническое задание на создание СЗИ ОИ.** Обоснование требований к СЗИ ОИ. Разработки технические решений по защите информации на ОИ. Обоснование состава СЗИ ОИ. Разработка концепции СЗИ ОИ. Разработка технического задания на создание СЗИ ОИ. **Проектирование СЗИ ОИ.** Эскизный проект СЗИ ОИ. Технический проект СЗИ ОИ. Рабочая документация на СЗИ ОИ. **Ввод в эксплуатацию СЗИ ОИ.** Порядок ввода СЗИ ОИ в эксплуатацию. Организационно-распорядительные документы, определяющие мероприятия по ЗИ в ходе эксплуатации ОИ; Предварительные испытания СЗИ ОИ. Организация аттестации ОИ по требованиям безопасности информации. **Проектирование систем (средств) информатизации в защищенном исполнении. Автоматизированные системы в защищенном исполнении (АСЗИ).** Автоматизированные системы (АС) – общие понятия. Основные компоненты АС. Свойства и показатели АС. Жизненный цикл АС. Состав системы защиты информации (СЗИ) АСЗИ. Функции СЗИ АСЗИ. Основные требования к СЗИ АСЗИ. **Порядок создания АСЗИ** Стадии и этапы создания АСЗИ (ГОСТ Р 51583-2014 и ГОСТ 34.601-90). Формирование требований к структуре АСЗИ. Разработка концепции АСЗИ. Техническое задание. Эскизный проект. Технический проект. Рабочая документация. Ввод в действие АСЗИ. Сопровождение АС. **Средства обеспечения надежности АСЗИ** Средства обеспечения надежности АСЗИ. Технологии создания отказоустойчивых систем. **Сертификация АСЗИ** Сертификация технических средств защиты информации. Сертификация криптографических средств защиты информации. Сертификация антивирусных программ. Специальные исследования и проверки СВТ. Специальные исследования СВТ на ПЭМИН. Специальные технические проверки СВТ. Сертификация АСЗИ. **Техническое обслуживание СЗИ ОИ и АСЗИ Основы организации эксплуатации СЗИ ОИ и АСЗИ** Термины и определения в области эксплуатации СЗИ и АСЗИ. Основные этапы эксплуатации СЗИ и АСЗИ, их краткая характеристика. Ввод в эксплуатацию и вывод из эксплуатации СЗИ и АСЗИ Порядок приема, выдачи и закрепления СЗИ и АСЗИ. Порядок ввода СЗИ в эксплуатацию. Порядок вывода из эксплуатации СЗИ и АСЗИ. Организация списания и утилизации СЗИ и АСЗИ. Обеспечение режима секретности при утилизации СЗИ и АСЗИ. Меры безопасности при эксплуатации СЗИ и АСЗИ Общие требования по обеспечению безопасности при эксплуатации СЗИ и АСЗИ. Меры безопасности при эксплуатации СЗИ и АСЗИ. Порядок допуска личного состава к самостоятельной работе со СЗИ. Виды, порядок и сроки инструктажей личного состава по технике безопасности. **Основы технического обслуживания СЗИ и АСЗИ** Роль и место системы технического обслуживания и ремонта в системе эксплуатации СЗИ и АСЗИ. Состав и содержание эксплуатационной документации на СЗИ и АСЗИ. Обеспечение режима секретности при эксплуатации и техническом обслуживании СЗИ. Организация технического обслуживания СЗИ и АСЗИ Задачи и виды технического обслуживания СЗИ и АСЗИ. Характеристика видов технического обслуживания СЗИ и АСЗИ. Контроль и проверка состояния СЗИ и АСЗИ. Организация технического обслуживания СЗИ и АСЗИ. Организация обновления программного обеспечения СЗИ и АСЗИ. Организация технического обслуживания технических средств защиты информации. Основы метрологического обеспечения средств защиты информации Общие сведения о метрологии и метрологическом обеспечении. Виды и методы измерений. Погрешности измерений. Виды средств измерений. Метрологические характеристики средств измерений. Классы точности средств измерений. Виды и периодичность поверок средств измерений. Организация поверок средств измерений. Калибровка средств измерений. Организация рекламационной работы и ремонта СЗИ и АСЗИ Организация рекламационной работы. Организация ремонта СЗИ и АСЗИ. **Контроль, диагностирование и восстановление программного обеспечения** Методы диагностирования программного обеспечения и СВТ. Средства диагностирования программного обеспечения и СВТ (AIDA64, OCCT, CPU-Z, GPU-Z, MSI Kombustor, MSI Afterburner, CrystalDiskInfo, Victoria HDD, HWiNFO и др). Средства восстановления программного обеспечения ([Acronis True Image](https://lumpics.ru/system-restore-software/#Acronis_True_Image), [Aomei Backupper Standard](https://lumpics.ru/system-restore-software/#Aomei_Backupper_Standard), [Macrium Reflect](https://lumpics.ru/system-restore-software/#Macrium_Reflect), [Windows Handy Backup](https://lumpics.ru/system-restore-software/#Windows_Handy_Backup), [Windows Repair](https://lumpics.ru/system-restore-software/#Windows_Repair) и др.). Организация восстановления программного обеспечения при сбоях. Неисправности СВТ, характерные особенности их проявления и методы восстановления работоспособности

Рекомендуемый перечень лабораторных работ:

1. Предварительное обследование объекта информатизации и обоснование необходимости создания СЗИ ОИ.

2. Формирование требований к СЗИ ОИ.

3. Разработка технического задания на СЗИ ОИ.

4. Разработка эскизного проекта СЗИ ОИ.

5. Разработка документации на СЗИ ОИ.

Рекомендуемый перечень основной литературы:

1. Проектирование информационных систем. Стандартизация: учеб. пособие / Т.В. Гвоздева, Б.А. Баллод. – 2-е изд., стер. – СПб: Лань, 2021. – 252 с.

2. Коваленко В.В. Проектирование информационных систем: учебное пособие. – М.: Форум, 2012. – 320 с.

3. Мельников Д.А. Информационная безопасность открытых систем: учебник. – М.: Флинта: Наука, 2014. – 448 с.

4. Программно-аппаратные средства защиты информации: учебное пособие. / В.А. Воеводин, А.В. Душкин, А.Н. Петухов, А.А. Хорев; под ред. А.А. Хорева. – М.: МИЭТ, 2021. – 280 с.

5. Программно-аппаратные средства защиты информации: учебно-методическое пособие. / А.В. Душкин, О.Р. Лукманова, А.Н. Петухов, А.А. Хорев; под ред. А.А. Хорева. – М.: МИЭТ, 2021. – 216 с.

6. Технические средства и методы защиты информации: учебник. / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков. – 7-е изд., испр. и доп. – М.: Горячая линия-Телеком, 2018. – 444 с.

7. Управление безопасностью критических информационных инфраструктур: учебное пособие / А.Н. Петухов, П.Л. Пилюгин, А.В. Душкин, Ю.А. Губсков; под ред. А.В. Душкина. – М.: МИЭТ, 2021. – 208 с.

8. Хорев А.А. Техническая защита информации: учебное пособие: В 3-х т. Т. 1: Технические каналы утечки информации. – М.: НПЦ «Аналитика», 2008. –   
436 с.

Перечень материально-технического обеспечения:

- лаборатория программно-аппаратных средств защиты информации;

- лаборатория технической защиты информации, оснащенная специализированным оборудованием по защите информации от утечки   
по акустическому, акустоэлектрическому каналам, каналу побочных электромагнитных излучений и наводок, техническими средствами контроля эффективности защиты информации от утечки по указанным каналам.

**Б.2.О.1. Производственная (преддипломная) практика**

Цель: выполнение выпускной квалификационной работы.

Задачи:

- осуществление сбора, обработки, анализа и систематизации научно-технической информации по теме выпускной квалификационной работы;

- выбор методик и средств решения поставленной задачи, разработка плана и графика подготовки выпускной квалификационной работы;

- оценка технических возможностей, подготовка рекомендаций по построению и проектирование отдельных элементов информационно-телекоммуникационной инфраструктуры с учетом обеспечения требований информационной безопасности, проведение экспериментальных исследований в соответствии с планом подготовки выпускной квалификационной работы;

- оформление пояснительной записки к выпускной квалификационной работе, подготовка доклада и презентации.

Формируемые компетенции: УК-1, УК-2, УК-4, УК-6, ОПК-1, ОПК-2, ОПК-3, ОПК-4, ОПК-5.

**5.5. Примерная рабочая программа воспитания**

Цели воспитательной работы:

- создание условий для активной жизнедеятельности обучающихся,   
их гражданского самоопределения, профессионального становления   
и индивидуально-личностной самореализации в созидательной деятельности   
для удовлетворения потребностей в нравственном, культурном, интеллектуальном, социальном и профессиональном развитии;

- подготовка творчески мыслящих и гармонично развитых специалистов, обладающих профессиональными навыками и высокими гражданскими качествами.

Задачи воспитательной работы:

- формирование уважительного отношения к закону, нормам коллективной жизни, развитие гражданской и социальной ответственности;

- воспитание внутренней потребности личности в здоровом образе жизни, ответственного отношения к природной и социокультурной среде;

- обеспечение развития личности и ее социально-психологической поддержки, формирование личностных качеств необходимых для эффективной профессиональной деятельности;

- выявление и поддержка талантливой молодежи, формирование организаторских навыков, творческого потенциала, вовлечение обучающихся   
в процессы саморазвития и самореализации;

- создание и совершенствование условий для личностного   
и профессионального формирования обучающихся в соответствии с моделью личности выпускника;

- разработка системы воспитательной деятельности, которая позволит достигать высокого уровня характеристик, предполагаемых в модели личности выпускника.

Результаты реализации программы воспитания:

- формирование системы компетенций на основе использования ресурсов учебной, внеучебной и социально-ориентированной деятельности;

- формирование духовных, социальных и профессиональных ценностей;

- обогащение личностного и социального опыта обучающихся;

- профессионально-личностная самореализация обучающихся.

Направления воспитательной работы изложены в таблице 3.

Таблица 3.

Направления воспитательной работы Организации

| № п/п | Направления  воспитательной работы | Воспитательные задачи |
| --- | --- | --- |
| 1 | Гражданско-правовое  и патриотическое воспитание, формирование патриотического сознания  и поведения обучающихся, уважения к закону | Формирование патриотического сознания и поведения обучающихся, уважения к закону и правопорядку, готовности к достойному служению обществу  и государству, нетерпимого отношения  к коррупционному поведению |
| 2 | Нравственное воспитание, межнациональные отношения и толерантность | Развитие духовно-нравственной культуры студента: повышение степени освоения личностью социального опыта, ценностей культурно-регионального сообщества, культуры, приобщение студентов к нравственным ценностям, развитие нравственных чувств; становление нравственной воли; побуждение к нравственному поведению;  Развитие культуры межнационального общения  и формирование установок на равнозначность  и равноценность каждого члена общества, социальная адаптация иностранных граждан, социальная адаптация лиц с ограниченными возможностями здоровья  и инвалидов |
| 3 | Профессиональная ориентация | Помощь в формировании критериев выбора индивидуальной траектории профессионального развития |
| 4 | Развитие добровольчества  и волонтерства | Поддержка добровольческих и волонтерских инициатив по всем направлениям (в сфере гражданско-патриотического воспитания, охраны природы, спорта, донорства и т.д.) |
| 5 | Культурно-творческое воспитание | Поддержка и развитие творческих способностей  и талантов обучающихся;  Создание условий для развития эстетического вкуса, повышения уровня культуры, приобщение к культурному наследию и традициям народов России |
| 6 | Физическое воспитание  и популяризация здорового образа жизни | Формирование навыков здорового образа жизни, массового спорта и физической культуры, профилактика вредных привычек |
| 7 | Информационно-воспитательная работа | Повышение культуры информационной безопасности в молодежной среде, противодействие распространению идеологии терроризма, экстремизма, национализма, ксенофобии |
| 8 | Развитие самоуправления обучающихся | Поддержка инициативы обучающихся в вопросах организации учебной и внеучебной жизни |
| 9 | Воспитательная работа  в рамках учебной деятельности – научно-образовательное воспитание | Содействие профессиональному самоопределению обучающихся, их профессиональному развитию;  Формирование исследовательского и критического мышления, мотивации к научно-исследовательской деятельности |

Основными функциями управления воспитательной работой выступают:

- планирование воспитательной работы на учебный год;

- организация воспитательной работы;

- анализ итогов воспитательной работы;

- контроль за исполнением управленческих решений   
по воспитательной работе;

- регулирование воспитательной работы.

Основным инструментом управления воспитательной работой Организации являются: Рабочая программа воспитательной работы, План воспитательной работы на учебный год, Концепция воспитательной деятельности (при наличии).

Реализация мероприятий воспитательной работы в Организации, мониторинг ее качества и анализ результатов реализуются поэтапно:

1 этап реализации программы воспитания обучающихся – формирование ценностно-смысловых основ профессиональной деятельности (1 курс):

- анализ портфолио (количество обучающихся, получивших почетные грамоты, благодарности, благодарственные письма за активную общественную работу, в сфере воспитательной деятельности);

- создание условий для формирования и исследования уровня удовлетворенности различными аспектами жизни обучающихся (анкетирование);

- создание условий для формирования студенческого самоуправления   
в студенческом коллективе и изучение динамики его развития (формирование старостата, анализ вовлеченности обучающихся в различные направления деятельности Студенческого совета, внеаудиторные мероприятия);

- изучение сформированности ценностных ориентиров, уровня ответственности, патриотических, гражданских качеств, толерантности   
в современных реалиях совместного сосуществования различных народов   
и национальностей в соответствии с общечеловеческими идеалами (анкетирование);

- популяризация здорового образа жизни, профилактика вредных привычек (анкетирование обучающихся).

2 этап реализации программы воспитания обучающихся – профессионализация (2-3 курс):

- анализ портфолио (количество обучающихся, получивших почетные грамоты, благодарности, сертификаты участников в мероприятиях профессиональной направленности, благодарственные письма за активную общественную работу, в сфере воспитательной деятельности);

- сформированность профессиональных ориентиров (анкетирование);

- оценка уровня правосознания, нетерпимости к коррупционному поведению, идеологии экстремизма, ксенофобии (анкетирование);

- оценка уровня понимания важности саморазвития, индивидуально- психологических свойств для себя и общества (анкетирование);

3 этап реализации программы воспитания обучающихся – формирование мотивации к профессиональной деятельности (4-5 курс):

- анализ портфолио (количество обучающихся, получивших почетные грамоты, благодарности, сертификаты участников в мероприятиях профессиональной направленности, благодарственные письма за активную общественную работу, в сфере воспитательной деятельности);

- исследование уровня готовности обучающихся к решению профессиональных задач (анкетирование преподавателей);

- анкетирование уровня оказания помощи в трудоустройстве;

- анализ карьерных устремлений выпускников;

- анализ уровня мотивации;

- выявление потребности в молодых специалистах (анкетирование работодателей).

Результаты анкетирования обобщаются отделом организации воспитательной работы, факультетами, обсуждаются коллегиальными органами управления Организации и являются основанием для совершенствования рабочей программы воспитания.

**5.6. Примерный календарный план воспитательной работы**

Календарный план воспитательной работы Организации включает перечень основных мероприятий по направлениям воспитательной работы.

Примерная форма плана представлена в таблице 4.

Таблица 4.

Примерная форма календарного плана воспитательной работы Организации

| Дата | Содержание и формы деятельности  *(наименование мероприятий, формы: например, учебная экскурсия (виртуальная экскурсия), дискуссия, проектная сессия, акция, концерт, деловая игра, студенческая конференция и т.д.*[[3]](#footnote-3) | Участники  *(курс, группа, члены кружка, секции, проектная команда  и т.п.)* | Место проведения | Ответственные |
| --- | --- | --- | --- | --- |
| СЕНТЯБРЬ | | | | |
| 1 | День знаний |  |  |  |
| 3 | День солидарности в борьбе с терроризмом |  |  |  |
|  | День города |  |  |  |
|  | Работа кураторов с первокурсниками |  |  |  |
| 13 | День программиста (256 день года) |  |  |  |
|  | Посвящение в студенты |  |  |  |
|  | Введение в профессию (специальность) |  |  |  |
|  | Посещение совета ветеранов ВОВ |  |  |  |
| 27 | Всемирный день туризма |  |  |  |
| 29 | День Интернета России |  |  |  |
| ОКТЯБРЬ | | | | |
| 1 | День пожилых людей |  |  |  |
| 16 | День отца |  |  |  |
| НОЯБРЬ | | | | |
| 4 | День народного единства |  |  |  |
| 7 | День проведения военного парада на Красной площади |  |  |  |
| 17 | Международный день студентов |  |  |  |
| 19 | День преподавателя высшей школы |  |  |  |
| 27 | День матери (последнее воскресенье месяца) |  |  |  |
| ДЕКАБРЬ | | | | |
| 3 | День неизвестного солдата |  |  |  |
| 4 | День информатики |  |  |  |
| 9 | День Героев Отечества |  |  |  |
| 12 | День Конституции Российской Федерации |  |  |  |
| ЯНВАРЬ | | | | |
| 1 | Новый год |  |  |  |
| 25 | «Татьянин день» (праздник студентов) |  |  |  |
| ФЕВРАЛЬ | | | | |
| 8 | День русской науки |  |  |  |
| 23 | День защитников Отечества |  |  |  |
|  | Мероприятия по направлению «Ценностные приоритеты современной молодежи» |  |  |  |
| МАРТ | | | | |
| 8 | Международный женский день |  |  |  |
| 14 | Международный день числа «ПИ» |  |  |  |
| 18 | День воссоединения Крыма с Россией |  |  |  |
|  | Мероприятия по пропаганде здорового образа жизни |  |  |  |
| АПРЕЛЬ | | | | |
|  | Участие во всероссийской акции «День единых действий» |  |  |  |
| 20 | День донора России |  |  |  |
|  | Донорская акция |  |  |  |
| 21 | День местного самоуправления |  |  |  |
| 29 | Всемирный день танцев |  |  |  |
| МАЙ | | | | |
| 1 | Праздник весны и труда |  |  |  |
| 7 | День Радио |  |  |  |
| 9 | День Победы |  |  |  |
|  | Всероссийская акция  «Бессмертный полк» |  |  |  |
| 24 | День славянской письменности и культуры |  |  |  |
| 26 | День российского предпринимательства |  |  |  |
| 31 | День без табака |  |  |  |
| ИЮНЬ | | | | |
| 1 | Международный день защиты детей |  |  |  |
| 5 | День эколога |  |  |  |
| 6 | Пушкинский день России |  |  |  |
| 12 | День России |  |  |  |
| 22 | День памяти и скорби |  |  |  |
|  | Ежегодная церемония награждения  «Студент года» и «Преподаватель года» |  |  |  |
| 27 | День молодежи России |  |  |  |
| ИЮЛЬ | | | | |
| 8 | День семьи, любви и верности |  |  |  |
| АВГУСТ | | | | |
| 22 | День Государственного Флага Российской Федерации |  |  |  |

**5.7. Рекомендации по разработке фондов оценочных средств   
для промежуточной аттестации**

Для каждой учебной дисциплины (модуля) Организация разрабатывает фонды оценочных средств.

ФОС может быть представлен в виде части рабочей программы учебной дисциплины (модуля), практики, в виде отдельного единого документа или комплекта документов.

ФОС должен включать в себя:

1. Перечень компетенций по учебной дисциплине (модулю), практике с указанием (при необходимости) этапов их формирования в процессе освоения образовательной программы.

2. Перечень индикаторов достижения соответствующих компетенций, включающий в себя индикаторы, предусмотренные ПООП, и индикаторы, определенные организацией самостоятельно (при необходимости).

3. Перечень форм и средств текущей и промежуточной аттестаций, используемых для оценивания индикаторов достижения компетенций. К ним могут относиться тесты, экзаменационные вопросы и вопросы для зачета, задачи, задания, кейсы, отчеты о лабораторных работах и прочие средства.

4. Описание шкал и процедур оценивания индикаторов достижения и соответствующих им компетенций.

Конкретная структура, состав и содержание ФОС разрабатываются и устанавливаются Организацией самостоятельно.

**5.8. Рекомендации по разработке программы государственной итоговой аттестации**

Программа ГИА включает в себя критерии оценивания ВКР и программу государственного экзамена (если Организация включила государственный экзамен в состав ГИА).

Программа ГИА может быть представлена в виде единого документа   
или комплекта документов.

Конкретная структура, состав и содержание программы ГИА разрабатываются и устанавливаются Организацией самостоятельно.

Программа ГИА должна включать в себя:

1. Перечень компетенций, выносимых на ГИА.

2. Перечень индикаторов достижения компетенций, выносимых на ГИА, включающий в себя индикаторы, предусмотренные ПООП, и индикаторы, определенные организацией самостоятельно (при необходимости).

3. Описание шкал и процедур оценивания индикаторов достижения и соответствующих им компетенций.

Программа государственного экзамена должна включать в себя вопросы и (или) задания, необходимые для оценивания индикаторов достижения компетенций, выносимых на государственный экзамен.

Для оценивания ВКР в программу ГИА рекомендуется включать следующие критерии:

1) Профессиональная группа критериев: степень актуальности тематики работы; степень раскрытия темы ВКР; корректность постановки задачи исследования и разработки; оригинальность и новизна полученных результатов, научных, конструкторских и технологических решений.

2) Справочно-информационная группа критериев: степень комплексности работы, использование в ней знаний дисциплин (модулей); использование информационных ресурсов Интернет; использование современных пакетов компьютерных программ и технологий.

3) Оформительская группа критериев: объем и качество выполнения графического материала.

4) Показатели защиты: качество защиты; уровень ответов.

5) Отзывы руководителя и рецензента: оценка руководителя; оценка рецензента.

**Раздел 6. ПРИМЕРНЫЕ УСЛОВИЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ ПО ОПОП**

**6.1. Общесистемные условия реализации программы специалитета**

Каждый обучающийся в течение всего периода обучения должен быть обеспечен индивидуальным неограниченным доступом к электронной информационно-образовательной среде Организации из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети Интернет (далее – сеть Интернет), как на территории Организации, так и вне ее. Условия   
для функционирования электронной информационно-образовательной среды могут быть созданы с использованием ресурсов иных организаций.

Электронная информационно-образовательная среда Организации должна обеспечивать:

доступ к учебным планам, рабочим программам дисциплин (модулей), программам практик, электронным учебным изданиям и электронным образовательным ресурсам, указанным в рабочих программах дисциплин (модулей), программах практик;

формирование электронного портфолио обучающегося, в том числе сохранение его работ и оценок за эти работы.

В случае реализации программы специалитета с применением электронного обучения, дистанционных образовательных технологий электронная информационно-образовательная среда Организации должна дополнительно обеспечивать:

фиксацию хода образовательного процесса, результатов промежуточной аттестации и результатов освоения программы специалитета;

проведение учебных занятий, процедур оценки результатов обучения, реализация которых предусмотрена с применением электронного обучения, дистанционных образовательных технологий;

взаимодействие между участниками образовательного процесса, в том числе синхронное и (или) асинхронное взаимодействия посредством сети Интернет.

Функционирование электронной информационно-образовательной среды обеспечивается соответствующими средствами информационно-коммуникационных технологий и квалификацией работников, ее использующих и поддерживающих. Функционирование электронной информационно-образовательной среды должно соответствовать законодательству Российской Федерации.

В федеральных государственных организациях, осуществляющих подготовку кадров в интересах обороны и безопасности государства, обеспечения законности   
и правопорядка, формирование, использование и эксплуатация электронной информационно-образовательной среды, доступ обучающихся к электронной информационно-образовательной среде, а также к современным профессиональным базам данных и информационным справочным системам, к компьютерной технике, подключенной к локальным сетям и (или) сети Интернет, организуются федеральным государственным органом, в ведении которого находятся соответствующие организации.

При реализации программы специалитета в сетевой форме требования   
к реализации программы специалитета обеспечиваются совокупностью ресурсов материально-технического и учебно-методического обеспечения, предоставляемого организациями, участвующими в реализации программы специалитета в сетевой форме.

При реализации программы специалитета Организация определяет отдельную кафедру или иное структурное подразделение, деятельность которого направлена   
на реализацию образовательных программ высшего образования по специальностям и направлениям подготовки, входящим в укрупненную группу специальностей   
и направлений подготовки 10.00.00 «Информационная безопасность».

**6.2. Требования к материально-техническому и учебно-методическому обеспечению программы специалитета**

Помещения должны представлять собой учебные аудитории для проведения учебных занятий, предусмотренных программой специалитета, оснащенные оборудованием и техническими средствами обучения, состав которых определяется в рабочих программах дисциплин (модулей).

Минимально необходимый для реализации программы специалитета перечень материально-технического обеспечения включает в себя специально оборудованные помещения для проведения учебных занятий, в том числе:

лаборатории:

- физики, оснащенную учебно-лабораторными стендами по механике, электричеству и магнетизму, электродинамике, оптике;

- электроники и схемотехники, оснащенную учебно-лабораторными стендами, средствами для измерения и визуализации частотных и временных характеристик сигналов, средствами для измерения параметров электрических цепей, средствами генерирования сигналов;

- цифровой обработки сигналов, оснащенную рабочими местами на базе вычислительной техники с поддержкой вычислений общего назначения   
на графических процессорах, платами цифровой обработки сигналов на базе сигнальных процессоров и программируемых логических интегральных схем, средствами разработки приложений для них;

- сетей и систем передачи информации, оснащенную рабочими местами   
на базе вычислительной техники, стендами сетей передачи информации   
с коммутацией пакетов и коммутацией каналов, структурированной кабельной системой, телекоммуникационным оборудованием, эмулятором активного сетевого оборудования, специализированным программным обеспечением для настройки телекоммуникационного оборудования;

- программно-аппаратных средств защиты информации, оснащенную антивирусными программными комплексами, аппаратными средствами аутентификации пользователя, программно-аппаратными комплексами защиты информации от несанкционированного доступа, включающими в том числе средства криптографической защиты информации;

- технической защиты информации, оснащенную специализированным оборудованием по защите информации от утечки по акустическому, акустоэлектрическому каналам, каналу побочных электромагнитных излучений   
и наводок, техническими средствами контроля эффективности защиты информации от утечки по указанным каналам;

- измерений в телекоммуникационных системах, оснащенную рабочими местами на базе вычислительной техники, структурированной кабельной системой, стендами для исследования параметров сетевого трафика, элементами телекоммуникационных систем с различными типами линий связи (проводных, беспроводных), комплектом измерительного оборудования для исследования параметров телекоммуникационных систем;

специально оборудованные кабинеты (классы, аудитории):

- информационных технологий, оснащенный рабочими местами на базе вычислительной техники и абонентскими устройствами, подключенными к сети Интернет с использованием проводных и (или) беспроводных технологий;

- научно-исследовательской работы обучающихся, курсового и дипломного проектирования, оснащенный рабочими местами на базе вычислительной техники   
с набором необходимых для проведения и оформления результатов исследований дополнительных аппаратных и (или) программных средств, а также комплектом оборудования для печати;

- аудиторию (защищаемое помещение) для проведения учебных занятий,   
в ходе которых до обучающихся доводится информация ограниченного доступа,   
не содержащая сведений, составляющих государственную тайну;

- специальную библиотеку (библиотеку литературы ограниченного доступа), предназначенную для хранения и обеспечения использования в образовательном процессе нормативных и методических документов ограниченного доступа.

для специализаций № 1 «Мониторинг в телекоммуникационных системах», № 2 «Системы представительской связи», № 3 «Сети специальной связи», № 4 «Системы и сети связи специального назначения», № 5 «Системы специальной связи и информации для органов государственной власти» также:

выделенное помещение (аудитория) для проведения учебных занятий, в ходе которых до обучающихся доводятся сведения, составляющие государственную тайну;

кабинет специальной техники, в том числе шифровальных средств;

кабинет огневой подготовки;

аудитория тактико-специальной (военно-профессиональной, специальной профессиональной) подготовки;

тир (для стрельбы из табельного оружия).

Компьютерные (специализированные) классы и лаборатории, если в них предусмотрены рабочие места на базе вычислительной техники, должны быть оборудованы современной вычислительной техникой из расчета одно рабочее место на каждого обучающегося при проведении занятий в данных классах (лабораториях).

Организация должна иметь лаборатории и (или) специально оборудованные кабинеты (классы, аудитории), обеспечивающие практическую подготовку выпускников в соответствии с каждой реализуемой специализацией программы специалитета.

Помещения для самостоятельной работы обучающихся должны быть оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду Организации.

Допускается частичная замена оборудования его виртуальными аналогами.

Организация должна быть обеспечена необходимым комплектом лицензионного и (или) свободно распространяемого программного обеспечения   
и сертифицированными средствами защиты информации, в том числе отечественного производства (состав определяется в рабочих программах дисциплин (модулей) и подлежит обновлению при необходимости).

При использовании в образовательном процессе печатных изданий библиотечный фонд должен быть укомплектован печатными изданиями из расчета не менее 0,25 экземпляра каждого из изданий, указанных в рабочих программах дисциплин (модулей), программах практик, на одного обучающегося из числа лиц, одновременно осваивающих соответствующую дисциплину (модуль), проходящих соответствующую практику.

Обучающимся должен быть обеспечен доступ (удаленный доступ), в том числе в случае применения электронного обучения, дистанционных образовательных технологий, к современным профессиональным базам данных   
и информационным справочным системам, состав которых определяется в рабочих программах дисциплин (модулей) и подлежит обновлению (при необходимости).

Доступ обучающихся к профессиональным базам данных и информационным справочным системам в федеральных государственных организациях, осуществляющих подготовку кадров в интересах обороны и безопасности государства, обеспечения законности и правопорядка, организуется федеральным государственным органом, в ведении которого находятся соответствующие организации.

Обучающиеся из числа инвалидов и лиц с ограниченными возможностями здоровья должны быть обеспечены печатными и (или) электронными образовательными ресурсами в формах, адаптированных к ограничениям   
их здоровья.

**6.3. Кадровые условия реализации программы специалитета**

Реализация программы специалитета обеспечивается педагогическими работниками Организации, а также лицами, привлекаемыми Организацией   
к реализации программы специалитета на иных условиях.

Квалификация педагогических работников Организации должна отвечать квалификационным требованиям, указанным в квалификационных справочниках   
и (или) профессиональных стандартах (при наличии).

В федеральных государственных организациях, осуществляющих подготовку кадров в интересах обороны и безопасности государства, обеспечения законности   
и правопорядка, квалификационные характеристики должностей руководителей и педагогических работников высшего образования и дополнительного профессионального образования определяются в соответствии с законодательством Российской Федерации.

Не менее 70 процентов численности педагогических работников Организации, участвующих в реализации программы специалитета, и лиц, привлекаемых Организацией к реализации программы специалитета на иных условиях (исходя   
из количества замещаемых ставок, приведенного к целочисленным значениям), должны вести научную, учебно-методическую и (или) практическую работу, соответствующую профилю преподаваемой дисциплины (модуля).

Не менее 3 процентов численности педагогических работников Организации, участвующих в реализации программы специалитета, и лиц, привлекаемых Организацией к реализации программы специалитета на иных условиях (исходя   
из количества замещаемых ставок, приведенного к целочисленным значениям), должны являться руководителями и (или) работниками иных организаций, осуществляющими трудовую деятельность в профессиональной сфере, соответствующей профессиональной деятельности, к которой готовятся выпускники (иметь стаж работы в данной профессиональной сфере не менее 3 лет).

Доля педагогических работников Организации (исходя из количества замещаемых ставок, приведенного к целочисленным значениям) должна составлять не менее 65 процентов от общего количества лиц, привлекаемых к реализации программы специалитета.

Не менее 55 процентов численности педагогических работников Организации, участвующих в реализации основных образовательных программ высшего образования, и лиц, привлекаемых к образовательной деятельности Организации   
на иных условиях (исходя из количества замещаемых ставок, приведенного   
к целочисленным значениям), должны иметь ученую степень (в том числе ученую степень, полученную в иностранном государстве и признаваемую в Российской Федерации) и (или) ученое звание (в том числе ученое звание, полученное   
в иностранном государстве и признаваемое в Российской Федерации).

В реализации программы специалитета должен принимать участие минимум один педагогический работник Организации, имеющий ученую степень или ученое звание по научной специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность» или по научной специальности, соответствующей направлениям подготовки кадров высшей квалификации   
по программам подготовки научно-педагогических кадров в адъюнктуре, входящим в укрупненную группу специальностей и направлений подготовки 10.00.00 «Информационная безопасность».

В федеральных государственных организациях, осуществляющих подготовку кадров в интересах обороны и безопасности государства, обеспечения законности   
и правопорядка, к педагогическим работникам с учеными степенями и (или) учеными званиями приравниваются преподаватели военно-профессиональных   
и специальных профессиональных дисциплин (модулей) без ученых степеней   
и (или) ученых званий, имеющие профильное высшее образование, опыт военной службы (службы в правоохранительных органах) в области и с объектами профессиональной деятельности, соответствующими программе магистратуры,   
не менее 10 лет, воинское (специальное) звание не ниже «майор» («капитан   
3 ранга»), а также имеющие боевой опыт или государственные (ведомственные) награды, или государственные (отраслевые) почетные звания, или государственные премии.

**6.4. Финансовые условия реализации программы специалитета**

Финансовое обеспечение реализации программы специалитета должно осуществляться в объеме не ниже значений базовых нормативов затрат на оказание государственных услуг по реализации образовательных программ высшего образования – программ специалитета и значений корректирующих коэффициентов к базовым нормативам затрат, определяемых Министерством науки и высшего образования Российской Федерации.

В Организации, в которой законодательством Российской Федерации предусмотрена военная или иная приравненная к ней служба, служба   
в правоохранительных органах, финансовое обеспечение реализации программы специалитета должно осуществляться в пределах бюджетных ассигнований федерального бюджета, выделяемых федеральному органу исполнительной власти, в ведении которого находится указанная Организация.

**6.5. Условия оценки качества образовательной деятельности и подготовки обучающихся по программе специалитета**

Качество образовательной деятельности и подготовки обучающихся   
по программе специалитета определяется в рамках системы внутренней оценки,   
а также системы внешней оценки, в которой Организация принимает участие   
на добровольной основе.

В целях совершенствования программы специалитета Организация   
при проведении регулярной внутренней оценки качества образовательной деятельности и подготовки обучающихся по программе специалитета привлекает работодателей и (или) их объединения, иных юридических и (или) физических лиц, включая педагогических работников Организации.

В рамках внутренней системы оценки качества образовательной деятельности по программе специалитета обучающимся предоставляется возможность оценивания условий, содержания, организации и качества образовательного процесса в целом и отдельных дисциплин (модулей) и практик.

Внешняя оценка качества образовательной деятельности по программе специалитета в рамках процедуры государственной аккредитации осуществляется   
с целью подтверждения соответствия образовательной деятельности по программе специалитета требованиям ФГОС ВО.

Внешняя оценка качества образовательной деятельности и подготовки обучающихся по программе специалитета может осуществляться в рамках профессионально-общественной аккредитации, проводимой работодателями,   
их объединениями, а также уполномоченными ими организациями, в том числе иностранными организациями, либо авторизованными национальными профессионально-общественными организациями, входящими в международные структуры, с целью признания качества и уровня подготовки выпускников отвечающими требованиям профессиональных стандартов (при наличии)   
и (или) требованиям рынка труда к специалистам соответствующего профиля.

В федеральных государственных организациях, осуществляющих подготовку кадров в интересах обороны и безопасности государства, обеспечения законности   
и правопорядка, внешняя оценка качества программы специалитета может осуществляться в рамках профессионально-общественной аккредитации, проводимой работодателями, их объединениями, а также уполномоченными   
ими организациями, с целью признания качества и уровня подготовки выпускников отвечающими требованиям профессиональных стандартов (при наличии)   
и (или) требованиям рынка труда к специалистам соответствующего профиля.

**Раздел 7. СПИСОК РАЗРАБОТЧИКОВ**

|  |  |
| --- | --- |
| Ф.И.О. разработчика | Должность |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Приложение 1.

Перечень профессиональных стандартов,   
соответствующих профессиональной деятельности   
выпускников, освоивших программу специалитета по специальности   
10.05.02 «Информационная безопасность телекоммуникационных систем»

|  |  |  |
| --- | --- | --- |
| №  п/п | Код профессионального стандарта | Наименование области профессиональной деятельности. Наименование профессионального стандарта |
| 06 Связь, информационные и коммуникационные технологии | | |
|  | 06.006 | Профессиональный стандарт «Специалист по радиосвязи  и телекоммуникациям», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 19 мая 2014 г. № 318н (зарегистрирован Министерством юстиции Российской Федерации 5 июня 2014 г., регистрационный № 32595), с изменением, внесенным приказом Министерства труда  и социальной защиты Российской Федерации от 12 декабря 2016 г. № 727н (зарегистрирован Министерством юстиции Российской Федерации 13 января 2017 г., регистрационный № 45230) |
|  | 06.007 | Профессиональный стандарт «Инженер-проектировщик  в области связи (телекоммуникаций)», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 16 ноября 2020 г. № 785н (зарегистрирован Министерством юстиции Российской Федерации 21 декабря 2020 г., регистрационный № 61610) |
|  | 06.018 | Профессиональный стандарт «Инженер связи (телекоммуникаций)», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 31 октября 2014 г. № 866н (зарегистрирован Министерством юстиции Российской Федерации 28 ноября 2014 г., регистрационный № 34971), с изменением, внесенным приказом Министерства труда и социальной защиты Российской Федерации от 12 декабря 2016 г. № 727н (зарегистрирован Министерством юстиции Российской Федерации 13 января 2017 г., регистрационный № 45230) |
|  | 06.023 | Профессиональный стандарт «Работник по представлению услуг телефонной, телеграфной и радиосвязи», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 16 ноября 2020 г. № 784н (зарегистрирован Министерством юстиции Российской Федерации 21 декабря 2020 г., регистрационный № 61653) |
|  | 06.027 | Профессиональный стандарт «Специалист  по администрированию сетевых устройств информационно-коммуникационных систем», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 5 октября 2015 г. № 686н (зарегистрирован Министерством юстиции Российской Федерации 30 октября 2015 г., регистрационный № 39568) |
|  | 06.030 | Профессиональный стандарт «Специалист по защите информации в телекоммуникационных системах и сетях», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 3 ноября 2016 г. № 608н (зарегистрирован Министерством юстиции Российской Федерации 25 ноября 2016 г., регистрационный № 44449) |
|  | 06.031 | Профессиональный стандарт «Специалист по автоматизации информационно-аналитической деятельности в сфере безопасности», утвержденный приказом Министерства труда  и социальной защиты Российской Федерации от 9 ноября 2016 г. № 611н (зарегистрирован Министерством юстиции Российской Федерации 25 ноября 2016 г., регистрационный № 44398) |
|  | 06.032 | Профессиональный стандарт «Специалист по безопасности компьютерных систем и сетей», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. № 598н (зарегистрирован Министерством юстиции Российской Федерации 28 ноября 2016 г., регистрационный № 44464) |
|  | 06.033 | Профессиональный стандарт «Специалист по защите информации в автоматизированных системах», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016 г. № 522н (зарегистрирован Министерством юстиции Российской Федерации 28 сентября 2016 г., регистрационный № 43857) |
|  | 06.034 | Профессиональный стандарт «Специалист по технической защите информации», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. № 599н (зарегистрирован Министерством юстиции Российской Федерации 25 ноября 2016 г., регистрационный № 44443) |
| 12 Обеспечение безопасности | | |
|  | 12.005 | Профессиональный стандарт, утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 25 декабря 2015 г. № 15с (зарегистрирован Министерством юстиции Российской Федерации 22 января 2016 г., регистрационный № 40706) |

Приложение 2.

Перечень обобщённых трудовых функций и трудовых функций,   
имеющих отношение к профессиональной деятельности выпускника программы специалитета   
по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем»

| **Код и наименование профессионального стандарта** | **Обобщенные трудовые функции** | | | **Трудовые функции** | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Код** | **Наименование** | **Уровень квалификации** | **Наименование** | **Код** | **Уровень (подуровень) квалификации** |
| 06.030 «Специалист по защите информации в телекоммуникационных системах и сетях» | A | Выполнение  комплекса мер по  обеспечению  функционирования  средств связи сетей электросвязи (за  исключением сетей  связи специального  назначения) и  средств их защиты от несанкционированного доступа | 5 | Установка программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты средств связи сетей электросвязи от несанкционированного доступа | A/01.5 | 5 |
| Обеспечение бесперебойной работы средств связи сетей электросвязи, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем их защиты от несанкционированного доступа | A/02.5 | 5 |
| Техническое обслуживание средств связи сетей электросвязи, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем их защиты от несанкционированного доступа | A/03.5 | 5 |
| B | Обеспечение защиты от несанкционированного доступа и компьютерных атак сооружений и средств связи сетей электросвязи (за исключением сетей связи специального назначения) в процессе их эксплуатации | 6 | Мониторинг функционирования средств связи сетей электросвязи, защищенности от несанкционированного доступа и компьютерных атак сооружений и средств связи сетей электросвязи | B/01.6 | 6 |
| Управление функционированием средств связи сетей электросвязи, защищенностью от несанкционированного доступа и компьютерных атак сооружений и средств связи сетей электросвязи | B/02.6 | 6 |
| Управление персоналом, обслуживающим сооружения и средств связи сетей электросвязи, а также программные, программно-аппаратные (в том числе криптографические) и технические средства и системы их защиты от несанкционированного доступа, средства для поиска признаков компьютерных атак в сетях электросвязи | B/03.6 | 6 |
| C | Обеспечение функционирования средств связи сетей связи специального назначения | 6 | Установка средств связи сетей связи специального назначения, включая средства криптографической защиты информации, средства для поиска признаков компьютерных атак в сетях электросвязи | C/01.6 | 6 |
| Обеспечение бесперебойной работы средств связи сетей связи специального назначения, включая средства криптографической защиты информации, средства для поиска признаков компьютерных атак в сетях электросвязи | C/02.6 | 6 |
| Ведение специального делопроизводства и технических документов в процессе эксплуатации средств связи сетей связи специального назначения, включая средства криптографической защиты информации | C/03.6 | 6 |
| D | Разработка средств защиты средств связи сетей электросвязи (за исключением сетей связи специального назначения) от несанкционированного доступа и компьютерных атак | 7 | Анализ угроз информационной безопасности в сетях электросвязи | D/01.7 | 7 |
| Разработка средств и систем защиты средств связи сетей электросвязи от несанкционированного доступа, средств для поиска признаков компьютерных атак в сетях электросвязи защищенных телекоммуникационных систем | D/02.7 | 7 |
| Проведение научно-исследовательских и опытно-конструкторских работ в сфере разработки средств и систем защиты средств связи сетей электросвязи от несанкционированного доступа, создания защищенных телекоммуникационных систем | D/03.7 | 7 |
| E | Обеспечение защиты средств связи сетей связи специального назначения от несанкционированного доступа | 7 | Организация функционирования сетей связи специального назначения и их средств связи | E/01.7 | 7 |
| Проведение научно-исследовательских и опытно-конструкторских работ в сфере разработки сетей связи специального назначения и их средств связи, включая средства криптографической защиты информации | E/02.7 | 7 |
| Контроль защищенности от несанкционированного доступа и функциональности сетей связи специального назначения | E/03.7 | 7 |
| F | Управление развитием средств и систем защиты средств связи сетей электросвязи от несанкционированного доступа | 7 | Управление рисками систем защиты сетей электросвязи от несанкционированного доступа | F/01.7 | 7 |
| 06.031 «Специалист по автоматизации информационно-аналитической деятельности в сфере безопасности» | C | Эксплуатация информационно-аналитических систем в защищенном исполнении | 7 | Обеспечение функционирования средств защиты информации в информационно-аналитических систем в защищенном исполнении | C/03.7 | 7 |
| D | Организационное управление в информационно-аналитических систем в защищенном исполнении | 7 | Организация работ по выполнению в информационно-аналитических системах в защищенном исполнении требований защиты информации ограниченного доступа | D/03.7 | 7 |
| 06.032 «Специалист по безопасности компьютерных систем и сетей» | B | Администрирование средств защиты информации в компьютерных системах и сетях | 6 | Администрирование подсистем защиты информации в операционных системах | B/01.6 | 6 |
| Администрирование программно-аппаратных средств защиты информации в компьютерных сетях | B/02.6 | 6 |
| Администрирование средств защиты информации прикладного и системного программного обеспечения | B/03.6 | 6 |
| C | Оценивание уровня безопасности компьютерных систем и сетей | 7 | Разработка требований по защите, формирование  политик безопасности компьютерных систем и сетей | C/02.7 | 7 |
| Проведение анализа безопасности компьютерных систем | C/03.7 | 7 |
| Проведение инструментального мониторинга защищенности компьютерных систем и сетей | C/05.7 | 7 |
| 06.033 «Специалист по защите информации в автоматизированных системах» | B | Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации | 6 | Администрирование систем защиты информации автоматизированных систем | B/02.6 | 6 |
| Управление защитой информации в автоматизированных системах | B/03.6 | 6 |
| Мониторинг защищенности информации в автоматизированных системах | B/05.6 | 6 |
| Аудит защищенности информации в автоматизированных системах | B/06.6 | 6 |
| C | Внедрение систем защиты информации автоматизированных систем | 6 | Установка и настройка средств защиты информации в автоматизированных системах | C/01.6 | 6 |
| Разработка организационно-распорядительных документов по защите информации в автоматизированных системах | C/02.6 | 6 |
| Анализ уязвимостей внедряемой системы защиты информации | C/03.6 | 6 |
| Внедрение организационных мер по защите информации в автоматизированных системах | C/04.6 | 6 |
| D | Разработка систем защиты информации автоматизированных систем | 7 | Разработка проектных решений по защите информации в автоматизированных системах | D/02.7 | 7 |
| Разработка эксплуатационной документации на системы защиты информации автоматизированных систем | D/03.7 | 7 |
| Разработка программных и программно-аппаратных средств для систем защиты информации автоматизированных систем | D/04.7 | 7 |
| 06.034 «Специалист по технической защите информации» | B | Проведение работ по установке и техническому обслуживанию защищенных технических средств обработки информации | 6 | Проведение работ по установке, настройке и испытаниям защищенных технических средств обработки информации | B/01.6 | 6 |
| F | Проектирование объектов в защищенном исполнении | 7 | Проектирование средств и систем информатизации в защищенном исполнении | F/01.7 | 7 |
| Проектирование систем защиты информации на объектах информатизации | F/02.7 | 7 |
| G | Проведение аттестации объектов на соответствие требованиям по защите информации | 7 | Проведение аттестации объектов вычислительной техники на соответствие требованиям по защите информации | G/01.7 | 7 |
| 06.006 «Специалист по радиосвязи и телекоммуникациям» | A | Эксплуатация и развитие коммутационных подсистем и сетевых платформ | 6 | Эксплуатация коммутационных подсистем и сетевых платформ | A/01.6 | 6 |
| Развитие коммутационных подсистем и сетевых платформ | A/02.6 | 6 |
| B | Эксплуатация и развитие сетей радиодоступа | 6 | Эксплуатация сетей радиодоступа | B/01.6 | 6 |
| Развитие сетей радиодоступа | B/02.6 | 6 |
| C | Эксплуатация и развитие транспортных сетей и сетей передачи данных, включая спутниковые системы | 6 | Эксплуатация транспортных сетей и сетей передачи данных | C/01.6 | 6 |
| Развитие транспортных сетей и сетей передачи данных | C/02.6 | 6 |
| Развитие спутниковых систем связи | C/03.6 | 6 |
| 06.007 «Инженер-проектировщик в области связи (телекоммуникаций)» | B | Разработка проектной и рабочей документации по оснащению объектов системами связи, телекоммуникационными системами и системами подвижной радиосвязи | 6 | Разработка схемы организации связи объекта, телекоммуникационной системы | B/01.6 | 6 |
| Разработка проектной документации на объект (систему) связи, телекоммуникационную систему | B/02.6 | 6 |
| Выполнение специальных расчетов | B/04.6 | 6 |
| Проектирование систем станций подвижной радиосвязи | B/06.6 | 6 |
| Проектирование транспортной сети подвижной радиосвязи | B/07.6 | 6 |
| 06.018 «Инженер связи (телекоммуникаций)» | A | Монтаж оборудования связи (телекоммуникаций), линейно-кабельных сооружений | 6 | Настройка, регулировка и испытания оборудования связи (телекоммуникаций) | A/02.6 | 6 |
| Тестирование оборудования, отработка режимов работы, контроль проектных параметров работы оборудования связи (телекоммуникаций) | A/03.6 | 6 |
| B | Эксплуатация оборудования связи (телекоммуникаций), линейно-кабельных сооружений | 6 | Проведение измерений параметров и проверки качества работы оборудования связи (телекоммуникаций) | B/01.6 | 6 |
| Проведение планово-профилактических работ | B/02.6 | 6 |
| Проведение ремонтно-восстанови тельных работ | B/03.6 | 6 |
| Мониторинг состояния оборудования, учет отказов оборудования, ведение документации | B/04.6 | 6 |
| C | Организация эксплуатации оборудования связи (телекоммуникаций) | 7 | Разработка технической документации по эксплуатации оборудования связи (телекоммуникаций) | C/02.7 | 7 |
| D | Планирование и оптимизация развития сети связи | 7 | Сбор и анализ исходных данных для развития и оптимизации сети связи | D/01.7 | 7 |
| Формирование плана развития сети связи | D/02.7 | 7 |
| Выработка и внедрение решений по оптимизации сети связи | D/03.7 | 7 |
| 06.023«Работник по представлению услуг телефонной, телеграфной и радиосвязи» | C | Обслуживание радиосвязи | 3 | Эксплуатационно-техническое обслуживание оборудования приемо-передающих радиостанций | C/02.3 | 3 |
| 06.027 «Специалист по администрированию сетевых устройств информационно-коммуникационных систем» | A | Администрирование процесса установки сетевых устройств инфокоммуникационных систем | 4 | Установка активных сетевых устройств | A/01.4 | 4 |
| Настройка программного обеспечения сетевых устройств | A/02.4 | 4 |
| Установка специальных средств управления сетевыми устройствами | A/03.4 | 4 |
| B | Администрирование процесса конфигурирования сетевых устройств и программного  обеспечения | 5 | Настройка параметров сетевых устройств и программного обеспечения согласно технологической политике организации | B/01.5 | 5 |
| Оценка эффективности конфигурации сетевых устройств с точки зрения производительности сети и защиты от несанкционированного доступа | B/03.5 | 5 |
| D | Администрирование процесса управления безопасностью сетевых устройств и программного обеспечения | 6 | Определение параметров безопасности и защиты программного обеспечения сетевых устройств | D/01.6 | 6 |
| Установка специальных средств управления безопасностью администрируемой сети | D/02.6 | 6 |
| Администрирование средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов) | D/03.6 | 6 |
| E | Проведение регламентных работ на сетевых устройствах и программном обеспечении инфокоммуникационной системы | 6 | Выполнение регламентных работ по поддержке операционных систем сетевых устройств инфокоммуникационной системы | E/01.6 | 6 |
| Восстановление параметров программного обеспечения сетевых устройств | E/03.6 | 6 |
| F | Администрирование процесса поиска и диагностики ошибок сетевых устройств и программного обеспечения | 7 | Устранение сбоев и отказов сетевых устройств и операционных систем | F/01.7 | 7 |
| Устранение ошибок сетевых устройств и операционных систем | F/03.7 | 7 |

Приложение 3.

Примерный учебный план   
программы специалитета по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем»

| Индекс | Наименование дисциплин (модулей), практик, аттестационных испытаний | Формы промежуточной аттестации | Трудоемкость | | | Примерное распределение по семестрам | | | | | | | | | | | Коды формируемых компетенций |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| з.е. | часы | |
| всего | контакт-ная работа | 1-й | 2-й | 3-й | 4-й | 5-й | 6-й | 7-й | 8-й | 9-й | 10-й | 11-й |
| **Б.1** | **Блок 1. Дисциплины (модули)** |  | **не менее 282** | **не менее 10480** | **не менее 5404** |  |  |  |  |  |  |  |  |  |  |  |  |
| **Б.1.О** | **Обязательная часть** |  | **не менее 221** | **не менее 8284** |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Б.1.О.1 | История (История России, Всеобщая история) | экзамен | 4 | 144 |  | x |  |  |  |  |  |  |  |  |  |  | ОПК-17 |
| Б.1.О.2 | Физическая культура | 2 зачета | 2 | 72 |  | x | x |  |  |  |  |  |  |  |  |  | УК-7 |
| Б.1.О.3 | Иностранный язык | 3 зачета,  экзамен | 11 | 396 |  | x | x | x | x |  |  |  |  |  |  |  | УК-4 |
| Б.1.О.4 | Экономика | экзамен | 4 | 144 |  |  |  |  | x |  |  |  |  |  |  |  | УК-10 |
| Б.1.О.5 | Философия | зачет,  экзамен | 5 | 180 |  |  |  |  |  | x | x |  |  |  |  |  | УК-1 |
| Б.1.О.6 | Безопасность жизнедеятельности | зачет | 3 | 108 |  |  |  |  |  |  |  | x |  |  |  |  | УК-8 |
| Б.1.О.7 | Управление проектами | зачет,  экзамен | 5 | 180 |  |  |  |  |  |  |  |  | x | x |  |  | УК-1, УК-2, УК-3, УК-6 |
|  | **Группа учебных дисциплин (модулей)  «Математические науки»** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Б.1.О.8 | Математический анализ | 3 экзамена | 15 | 540 |  | x | x | x |  |  |  |  |  |  |  |  | ОПК-3 |
| Б.1.О.9 | Теория вероятностей и математическая статистика | зачет,  экзамен | 6 | 216 |  |  |  |  | x | x |  |  |  |  |  |  | ОПК-3 |
| Б.1.О.10 | Алгебра и геометрия | зачет,  экзамен | 5 | 180 |  | x | x |  |  |  |  |  |  |  |  |  | ОПК-3 |
| Б.1.О.11 | Дискретная математика | экзамен | 4 | 144 |  |  |  | x |  |  |  |  |  |  |  |  | ОПК-3 |
|  | **Группа учебных дисциплин (модулей)  «Физико-технические основы функционирования телекоммуникационных систем»** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Б.1.О.12 | Физика | 3 экзамена | 18 | 648 |  | x | x | x |  |  |  |  |  |  |  |  | ОПК-4 |
| Б.1.О.13 | Электроника и схемотехника | зачет,  экзамен | 8 | 288 |  |  |  | x | x |  |  |  |  |  |  |  | ОПК-4 |
| Б.1.О.14 | Теория электросвязи (Теория электрических цепей, Теория радиотехнических сигналов, Теория электрической связи, Теория информации и кодирования) | 4 экзамена | 20 | 720 |  |  |  |  | x | x | x | x |  |  |  |  | ОПК-11 |
| Б.1.О.15 | Антенны и распространение радиоволн | зачет с оценкой | 4 | 144 |  |  |  |  |  | x |  |  |  |  |  |  | ОПК-11 |
| Б.1.О.16 | Цифровая обработка сигналов | зачет с оценкой | 4 | 144 |  |  |  |  |  |  | x |  |  |  |  |  | ОПК-11 |
|  | **Группа учебных дисциплин (модулей)  «Информационные технологии  и программирование»** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Б.1.О.17 | Языки программирования | 2 зачета,  экзамен | 10 | 360 |  | x | x | x |  |  |  |  |  |  |  |  | ОПК-2,  ОПК-7 |
| Б.1.О.18 | Методы программирования | экзамен | 4 | 144 |  |  |  |  | x |  |  |  |  |  |  |  | ОПК-7 |
| Б.1.О.19 | Прикладные информационные технологии | экзамен | 5 | 180 |  |  |  |  |  | x |  |  |  |  |  |  | ОПК-2 |
|  | **Группа учебных дисциплин (модулей)  «Телекоммуникационные технологии»** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Б.1.О.20 | Сети и системы передачи информации | 2 экзамена,  курсовая работа | 8 | 288 |  |  |  |  |  |  | x | x |  |  |  |  | ОПК-13,  ОПК-14 |
| Б.1.О.21 | Аппаратные средства телекоммуникационных систем | экзамен | 5 | 180 |  |  |  |  |  |  |  | x |  |  |  |  | ОПК-14 |
| Б.1.О.22 | Измерения в телекоммуникационных системах | экзамен | 4 | 144 |  |  |  |  |  |  |  |  | x |  |  |  | ОПК-12,  ОПК-15 |
| Б.1.О.23 | Моделирование систем и сетей телекоммуникаций | экзамен,  курсовая работа | 5 | 180 |  |  |  |  |  |  |  |  |  | x |  |  | ОПК-12 |
|  | **Группа учебных дисциплин (модулей)  «Методы и средства обеспечения информационной безопасности телекоммуникационных систем»** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Б.1.О.24 | Основы информационной безопасности | зачет | 3 | 108 |  |  | x |  |  |  |  |  |  |  |  |  | ОПК-1 |
| Б.1.О.25 | Организационное и правовое обеспечение информационной безопасности | зачет,  экзамен | 5 | 180 |  |  |  |  |  |  | x | x |  |  |  |  | ОПК-5,  ОПК-6 |
| Б.1.О.26 | Защита информации от утечки по техническим каналам | экзамен | 5 | 180 |  |  |  |  |  |  |  | x | x |  |  |  | ОПК-6,  ОПК-9 |
| Б.1.О.27 | Методы и средства криптографической защиты информации | экзамен | 5 | 180 |  |  |  |  |  |  |  |  | x |  |  |  | ОПК-10 |
| Б.1.О.28 | Программно-аппаратные средства защиты информации телекоммуникационных систем | экзамен | 5 | 180 |  |  |  |  |  |  |  |  | x |  |  |  | ОПК-9 |
| Б.1.О.29 | Проектирование защищенных телекоммуникационных систем | экзамен | 5 | 180 |  |  |  |  |  |  |  |  |  | x |  |  | ОПК-8,  ОПК-16 |
| Б.1.О.30 | Комплексное обеспечение защиты информации телекоммуникационных систем | экзамен | 5 | 180 |  |  |  |  |  |  |  |  |  |  | x |  | ОПК-6,  ОПК-13,  ОПК-15 |
|  | **Дисциплины (модули) образовательной организации (при необходимости)** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | **Элективные дисциплины (модули) образовательной организации** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Элективные дисциплины по физической культуре и спорту |  | 0 | не менее 328 |  |  |  |  |  |  |  |  |  |  |  |  | УК-7 |
| **Б.1.С** | **Дисциплины (модули) специализации** |  | **не менее 27** | **не менее 972** | **не менее 486** |  |  |  |  |  |  | **x** | **x** | **x** | **x** |  |  |
| *Б.1.С.1* | *специализация № 1 «Мониторинг в телекоммуникационных системах»* |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Дисциплины (модули) определяются квалификационными требованиями к военно-профессиональной подготовке, специальной профессиональной подготовке выпускников, устанавливаемыми федеральным государственным органом, в ведении которого находятся соответствующие образовательные организации. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| *Б.1.С.2* | *специализация № 2 «Системы представительской связи»* |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Дисциплины (модули) определяются квалификационными требованиями к военно-профессиональной подготовке, специальной профессиональной подготовке выпускников, устанавливаемыми федеральным государственным органом, в ведении которого находятся соответствующие образовательные организации. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| *Б.1.С.3* | *специализация № 3 «Сети специальной связи»* |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Дисциплины (модули) определяются квалификационными требованиями к военно-профессиональной подготовке, специальной профессиональной подготовке выпускников, устанавливаемыми федеральным государственным органом, в ведении которого находятся соответствующие образовательные организации. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| *Б.1.С.4* | *специализация № 4 «Системы и сети связи специального назначения»* |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Дисциплины (модули) определяются квалификационными требованиями к военно-профессиональной подготовке, специальной профессиональной подготовке выпускников, устанавливаемыми федеральным государственным органом, в ведении которого находятся соответствующие образовательные организации. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| *Б.1.С.5* | *специализация № 5 «Системы специальной связи и информации для органов государственной власти»* |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Дисциплины (модули) определяются квалификационными требованиями к военно-профессиональной подготовке, специальной профессиональной подготовке выпускников, устанавливаемыми федеральным государственным органом, в ведении которого находятся соответствующие образовательные организации. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| *Б.1.С.6* | *специализация № 6 «Информационная безопасность аэрокосмических телекоммуникационных систем»* |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Б.1.С.6.1 | Телекоммуникационные системы комплексов координатно-временного обеспечения | экзамен | 4 | 144 |  |  |  |  |  |  |  |  |  |  |  |  | ОПК-6.1 |
| Б.1.С.6.2 | Проектирование защищенных телекоммуникационных систем в контуре управления космическим аппаратом | экзамен | 5 | 180 |  |  |  |  |  |  |  |  |  |  |  |  | ОПК-6.1 |
| Б.1.С.6.3 | Протоколы сетевого взаимодействия объектов аэрокосмического и наземного сегментов телекоммуникационной системы | экзамен | 6 | 216 |  |  |  |  |  |  |  |  |  |  |  |  | ОПК-6.2 |
| Б.1.С.6.4 | Защита информационных процессов в телекоммуникационных сетях обеспечения функционирования летательных аппаратов | экзамен | 6 | 216 |  |  |  |  |  |  |  |  |  |  |  |  | ОПК-6.2 |
| Б.1.С.6.5 | Методы защиты радиолиний аэрокосмических телекоммуникационных систем с использованием перспективных сигнально-кодовых конструкций | экзамен | 6 | 216 |  |  |  |  |  |  |  |  |  |  |  |  | ОПК-6.3 |
|  | Дисциплины (модули) образовательной организации (при необходимости) |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| *Б.1.С.7* | *специализация № 7 «Разработка защищенных телекоммуникационных систем»* |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Б.1.С.7.1 | Разработка аппаратного и программного обеспечения узлов и устройств защищенных телекоммуникационных систем | экзамен | 4 | 144 |  |  |  |  |  |  |  |  |  |  |  |  | ОПК-7.1 |
| Б.1.С.7.2 | Управление информационной безопасностью телекоммуникационных систем | зачет,  экзамен | 9 | 324 |  |  |  |  |  |  |  |  |  |  |  |  | ОПК-7.2 |
| Б.1.С.7.3 | Защита программных средств защищенных телекоммуникационных систем | экзамен | 4 | 144 |  |  |  |  |  |  |  |  |  |  |  |  | ОПК-7.3 |
|  | Дисциплины (модули) образовательной организации (при необходимости) |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| *Б.1.С.8* | *специализация № 8 «Защита информации в радиосвязи и телерадиовещании»* |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Б.1.С.8.1 | Системы радиосвязи и сети телерадиовещания | экзамен | 9 | 324 |  |  |  |  |  |  |  |  |  |  |  |  | ОПК-8.1 |
| Б.1.С.8.2 | Устройства приема и обработки сигналов в защищенных системах радиосвязи | экзамен | 9 | 324 |  |  |  |  |  |  |  |  |  |  |  |  | ОПК-8.2 |
| Б.1.С.8.3 | Защита информации в системах радиосвязи и телерадиовещания | экзамен | 9 | 324 |  |  |  |  |  |  |  |  |  |  |  |  | ОПК-8.3 |
|  | Дисциплины (модули) образовательной организации (при необходимости) |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| *Б.1.С.9* | *специализация № 9 «Управление безопасностью телекоммуникационных систем и сетей»* |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Б.1.С.9.1 | Менеджмент информационной безопасности телекоммуникационных систем и сетей | экзамен | 6 | 216 |  |  |  |  |  |  |  |  |  |  |  |  | ОПК-9.1 |
| Б.1.С.9.2 | Правила и процедуры по обеспечению информационной безопасности телекоммуникационных систем и сетей | экзамен | 5 | 180 |  |  |  |  |  |  |  |  |  |  |  |  | ОПК-9.2 |
| Б.1.С.9.3 | Обеспечение устойчивости телекоммуникационных систем и сетей | зачет | 3 | 108 |  |  |  |  |  |  |  |  |  |  |  |  | ОПК-9.2 |
| Б.1.С.9.4 | Мониторинг безопасности телекоммуникационных систем и сетей | экзамен | 6 | 216 |  |  |  |  |  |  |  |  |  |  |  |  | ОПК-9.3 |
|  | Дисциплины (модули) образовательной организации (при необходимости) |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| *Б.1.С.10* | *специализация № 10 «Информационная безопасность мультисервисных телекоммуникационных сетей и систем на транспорте» (по видам)* |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Б.1.С.10.1 | Квантовая криптография в телекоммуникационных системах и сетях транспорта | экзамен | 8 | 288 |  |  |  |  |  |  |  |  |  |  |  |  | ОПК-10.1 |
| Б.1.С.10.2 | Информационная безопасность и защита информации в интегрированных телекоммуникационных и корпоративных сетях транспорта | экзамен | 9 | 324 |  |  |  |  |  |  |  |  |  |  |  |  | ОПК-10.2 |
| Б.1.С.10.3 | Специальные измерения и техническая диагностика в защищенных сетях транспорта | экзамен | 10 | 360 |  |  |  |  |  |  |  |  |  |  |  |  | ОПК-10.3 |
|  | Дисциплины (модули) образовательной организации (при необходимости) |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| *Б.1.С.11* | *специализация № 11 «Системы подвижной цифровой защищенной связи»* |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Б.1.С.11.1 | Основы цифровых телекоммуникационных сетей | 2 экзамена | 10 | 360 |  |  |  |  |  |  |  |  |  |  |  |  | ОПК-11.1 |
| Б.1.С.11.2 | Свойства беспроводных каналов связи | экзамен | 3 | 108 |  |  |  |  |  |  |  |  |  |  |  |  | ОПК-11.1,  ОПК-11.3 |
| Б.1.С.11.3 | Беспроводные системы связи и их безопасность | экзамен | 6 | 216 |  |  |  |  |  |  |  |  |  |  |  |  | ОПК-11.3 |
| Б.1.С.11.4 | Системы позиционирования подвижных объектов | зачет | 3 | 108 |  |  |  |  |  |  |  |  |  |  |  |  | ОПК-11.3 |
| Б.1.С.11.5 | Алгоритмы идентификации динамических моделей криптосистем | экзамен | 5 | 180 |  |  |  |  |  |  |  |  |  |  |  |  | ОПК-11.2 |
|  | Дисциплины (модули) образовательной организации (при необходимости) |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| *Б.1.С.12* | *специализация № 12 «Техническая защита информации информационно-телекоммуникационных систем»* |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Б.1.С.12.1 | Защита информации от утечки по техническим каналам. Дополнительные главы | экзамен | 7 | 252 |  |  |  |  |  |  |  |  |  |  |  |  | ОПК-12.1,  ОПК-12.2,  ОПК-12.3 |
| Б.1.С.12.2 | Программно-аппаратные средства защиты информации. Дополнительные главы | экзамен | 8 | 288 |  |  |  |  |  |  |  |  |  |  |  |  | ОПК-12.1,  ОПК-12.2,  ОПК-12.3 |
| Б.1.С.12.3 | Аттестация объектов информатизации | экзамен | 5 | 180 |  |  |  |  |  |  |  |  |  |  |  |  | ОПК-12.1,  ОПК-12.2,  ОПК-12.3 |
| Б.1.С.12.4 | Проектирование систем защиты объектов информатизации | экзамен | 5 | 180 |  |  |  |  |  |  |  |  |  |  |  |  | ОПК-12.1,  ОПК-12.2 |
|  | Дисциплины (модули) образовательной организации (при необходимости) |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Б.1.В** | **Часть, формируемая участниками образовательных отношений  (распределение дисциплин (модулей) по периодам обучения определяется образовательной организацией самостоятельно)** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | **Дисциплины (модули) образовательной организации (при необходимости)** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | **Элективные дисциплины (модули) образовательной организации  (при необходимости)** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Б.2** | **Блок 2. Практика** |  | **не менее 27** | **не менее 972** | **не менее 486** |  |  |  |  |  |  |  |  |  |  |  |  |
| **Б.2.О** | **Обязательная часть** |  | **не менее 27** | **не менее 972** |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Б.2.О.1 | Производственная (преддипломная) практика |  | не менее 15 | не менее 540 |  |  |  |  |  |  |  |  |  |  | x | x | УК-4, УК-6,  ОПК-8,  ОПК-13,  ОПК-16 |
|  | Учебная практика (тип (типы) определяются образовательной организацией) (при необходимости) |  |  |  |  |  | x | x | x | x | x | x | x | x | x |  |  |
|  | Производственная практика (тип (типы) определяются образовательной организацией) (при необходимости) |  |  |  |  |  | x | x | x | x | x | x | x | x | x |  |  |
| **Б.2.В** | **Часть, формируемая участниками образовательных отношений** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Учебная практика (тип (типы) определяются образовательной организацией) (при необходимости) |  |  |  |  |  | x | x | x | x | x | x | x | x | x |  |  |
|  | Производственная практика (тип (типы) определяются образовательной организацией) (при необходимости) |  |  |  |  |  | x | x | x | x | x | x | x | x | x |  |  |
| **Б.3** | **Блок 3. Государственная итоговая аттестация** |  | **6** | **216** |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Б.3.О** | **Обязательная часть** |  | **6** | **216** |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Б.3.О.1 | Защита выпускной квалификационной работы |  | 6 | 216 |  |  |  |  |  |  |  |  |  |  |  | x |  |
|  | **Итого по образовательной программе** |  | **330** | **12208** |  | **x** | **x** | **x** | **x** | **x** | **x** | **x** | **x** | **x** | **x** | **x** |  |

Примечания:

1. Образовательная организация в пределах требований, установленных ФГОС, при формировании образовательной программы высшего образования в отношении учебных дисциплин (модулей) и практик, указанных в настоящем примерном учебном плане, вправе: конкретизировать наименование; уменьшать, но не более чем на 2 з.е. и не ниже 3 з.е., а также увеличивать трудоемкость; устанавливать периоды обучения, в которых изучается учебная дисциплина (модуль) или практика, а также формы промежуточной аттестации по их окончании; разделять учебные дисциплины (модули) при условии сохранения общей трудоемкости   
и индикаторов достижения формируемых компетенций, установленных примерной основной образовательной программой для исходной учебной дисциплины (модуля).

2. Федеральные государственные образовательные организации, находящиеся в ведении федеральных государственных органов, указанных в части 1 статьи 81 Федерального закона от 29 декабря 2012 г. «Об образовании в Российской Федерации»,   
при формировании образовательной программы высшего образования в целях реализации квалификационных требований   
к военно-профессиональной подготовке, специальной профессиональной подготовке выпускников, устанавливаемых федеральным государственным органом, в ведении которого они находятся, в отношении учебных дисциплин (модулей), указанных в настоящем примерном учебном плане, вправе: изменять наименование и трудоемкость в пределах требований, установленных ФГОС.

Приложение 4.

Примерный календарный учебный график   
программы специалитета по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем»

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Месяцы | Сентябрь | | | |  | Октябрь | | |  | Ноябрь | | | | Декабрь | | | |  | Январь | | |  | Февраль | | |  | Март | | | |  | Апрель | | |  | Май | | | | Июнь | | | |  | Июль | | |  | Август | | | |
| Недели | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50 | 51 | 52 |
| **1 курс** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | ээ | ээ | кк | кк |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | ээ | ээ | ээ | ээ | кк | кк | кк | кк | кк | кк | кк | кк | кк | кк |
| **2 курс** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | ээ | ээ | ээ | кк | кк |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | ээ | ээ | ээ | ээ | кк | кк | кк | кк | кк | кк | кк | кк | кк | кк |
| **3 курс** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | ээ | ээ | ээ | ээ | кк | кк |  |  |  |  |  |  |  |  |  |  |  |  | ээ | ээ | ээ | пп | пп | пп | пп | кк | кк | кк | кк | кк | кк | кк | кк | кк | кк |
| **4 курс** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | ээ | ээ | ээ | ээ | кк | кк |  |  |  |  |  |  |  |  |  |  |  |  | ээ | ээ | ээ | пп | пп | пп | пп | кк | кк | кк | кк | кк | кк | кк | кк | кк | кк |
| **5 курс** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | ээ | ээ | ээ | кк | кк |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | ээ | ээ | ээ | ээ | кк | кк | кк | кк | кк | кк | кк | кк | кк | кк |
| **6 курс** |  |  |  |  |  |  |  | пп | пп | пп | пп | пп | пп | пп | пп | пп | пп | гг | гг | гг | гг | кк | кк |  | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Обозначения:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  | э |  |  |  |  | г |  |  |  |  | п |  |  |  |  | к |  |  |
| теоретическое обучение | | | | | экзаменационные сессии | | | | | итоговая государственная аттестация | | | | | практика | | | | | каникулы | | | | |
|  |  |  |  |  |  |  |  |  |  |

1. Федеральные государственные образовательные организации, осуществляющие подготовку кадров в интересах обороны и безопасности государства, обеспечения законности и правопорядка, находящиеся в ведении федеральных государственных органов, указанных в части 1 статьи 81 Федерального закона   
   от 29 декабря 2012 г. «Об образовании в Российской Федерации», при формировании образовательной программы высшего образования устанавливают индикаторы достижения компетенции самостоятельно на основе квалификационных требований к военно-профессиональной подготовке, специальной профессиональной подготовке выпускников, устанавливаемых федеральным государственным органом, в ведении которого они находятся [↑](#footnote-ref-1)
2. В федеральных государственных организациях, осуществляющих подготовку кадров в интересах обороны и безопасности государства, обеспечения законности   
   и правопорядка, дисциплина (модуль) может быть исключена. [↑](#footnote-ref-2)
3. В Календарном плане указаны государственные праздники Российской Федерации. В него также должны быть включены ключевые даты, которые значимы на уровне субъекта Российской Федерации, а также для отраслей, под нужды которых осуществляется подготовка кадров в образовательной организации. [↑](#footnote-ref-3)