**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

**10.05.03 Информационная безопасность автоматизированных 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 НАПРАВЛЕНИЯ ПОДГОТОВКИ (СПЕЦИАЛЬНОСТИ)

3.1. Направленности (профили) образовательных программ в рамках направления подготовки (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. Примерная рабочая программа воспитания

5.5. Примерный календарный план воспитательной работы

5.6. Примерные программы дисциплин (модулей) и практик

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 10.05.03 «Информационная безопасность автоматизированных систем»

Приложение 2. Перечень обобщённых трудовых функций и трудовых функций, имеющих отношение к профессиональной деятельности выпускника программ специалитета по направлению подготовки (специальности) 10.05.03 «Информационная безопасность автоматизированных систем»

Приложение 3. Примерный календарный учебный график программы специалитета по направлению подготовки (специальности) 10.05.03 «Информационная безопасность автоматизированных 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 10.05.03 «Информационная безопасность автоматизированных систем».

ПООП предназначена для разработки и реализации основных профессиональных образовательных программ высшего образования на основе федерального государственного образовательного стандарта высшего образования – специалитет по специальности 10.05.03 «Информационная безопасность автоматизированных систем», утвержденного приказом Минобрнауки России  
от 26 ноября 2020 г. № 1457, зарегистрированного в Минюсте 17 февраля 2021 года, рег. номер 62535 (далее – ОПОП, образовательная программа) и с учётом профессиональных стандартов, сопряжённых с профессиональной деятельностью выпускников.

## 1.2. Нормативные документы

* Федеральный закон от 29 декабря 2012 года № 273-ФЗ «Об образовании в Российской Федерации»;
* Федеральный государственный образовательный стандарт высшего образования – специалитет по специальности 10.05.03 «Информационная безопасность автоматизированных систем», утвержденный приказом Минобрнауки России от 26 ноября 2020 г. № 1457, зарегистрированного в Минюсте 17 февраля 2021 года, рег. номер 62535 (далее – ФГОС ВО);
* 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 года № 301 (далее – Порядок организации образовательной деятельности);
* 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;
* Положение о практике обучающихся, осваивающих основные профессиональные образовательные программы высшего образования, утвержденное приказом Минобрнауки России от 5 августа 2020 г. № 885/390.

## 1.3. Перечень сокращений, используемых в тексте ПООП

|  |  |  |
| --- | --- | --- |
| з.е. | – | зачетная единица; |
| ОПК | – | общепрофессиональная компетенция; |
| ОПОП | – | основная профессиональная образовательная программа; |
| Организация | – | организация, осуществляющая образовательную деятельность по специальности *(указывается код и наименование специальности)*; |
| ОТФ | – | обобщённая трудовая функция; |
| ПД | – | профессиональная деятельность; |
| ПК | – | профессиональная компетенция; |
| ПС | – | профессиональный стандарт; |
| ПООП | – | примерная основная образовательная программа по специальности *(указывается код и наименование специальности)*; |
| программа специалитета | – | основная образовательная программа высшего образования – программа специалитета *(указывается код и наименование специальности)*; |
| 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. |
| ФУМО |  | федеральное учебно-методическое объединение |
| 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 обеспечения безопасности информации в автоматизированных системах);

12 Обеспечение безопасности (в сфере обеспечения безопасности информации в автоматизированных системах, обладающих информационно-технологическими ресурсами, подлежащими защите);

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 10.05.03 «Информационная безопасность автоматизированных систем»

автоматизированные системы, функционирующие в условиях существования угроз в информационной сфере и обладающие информационно-технологическими ресурсами, подлежащими защите;

информационные технологии, формирующие информационную инфраструктуру в условиях существования угроз в информационной сфере и задействующие информационно-технологические ресурсы, подлежащие защите;

технологии обеспечения информационной безопасности автоматизированных систем;

системы управления информационной безопасностью автоматизированных систем.

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

Перечень профессиональных стандартов, соотнесенных с ФГОС ВО по специальности 10.05.03 «Информационная безопасность автоматизированных систем», приведен в приложении 1.

Перечень обобщённых трудовых функций и трудовых функций, имеющих отношение к профессиональной деятельности выпускника программ специалитета по специальности 10.05.03 «Информационная безопасность автоматизированных 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 10.05.03 «Информационная безопасность автоматизированных 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 10.05.03 «Информационная безопасность автоматизированных 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) профильного профессионального стандарта 06.033 Специалист по защите информации в автоматизированных системах |
| --- | --- | --- |
| *01 Образование и наука (в сфере научных исследований)* | *экспериментально-исследовательский* | С/01.6 - Установка и настройка средств защиты информации в автоматизированных системах |
| *научно-исследовательский* | В/03.6 - Управление защитой информации в автоматизированных системах  Е/04.8 - Моделирование защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации.  D/03.7 - Разработка предложений по развитию системы безопасности и реализация мер по совершенствованию безопасности значимых объектов критической информационной инфраструктуры критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| *06 Связь, информационные и коммуникационные технологии (в сфере обеспечения безопасности информации в автоматизированных системах)* | *проектный* | D/01.7 – Тестирование систем защиты информации автоматизированных систем  D/02.7 – Разработка проектных решений по защите информации в автоматизированных системах  D/03.7 - Разработка эксплуатационной документации на системы защиты информации автоматизированных систем.  D/04.7 - Разработка программных и программно-аппаратных средств для систем защиты информации автоматизированных систем Е/01.8 - Обоснование необходимости защиты информации в автоматизированной системе;С/03.7 - Проведение анализа безопасности компьютерных систем; В/03.6 - Администрирование средств защиты информации прикладного и системного программного обеспечения |
| *контрольно-аналитический* | В/01.6 - Диагностика систем защиты информации автоматизированных систем  В/05.6 - Мониторинг защищенности информации в автоматизированных системах  B/06.6 - Аудит защищенности информации в  автоматизированных системах  С/03.6 – Анализ уязвимостей внедряемой системы защиты информации  D/01.7 – Тестирование систем защиты информации автоматизированных систем  С/02.7 Разработка требований по защите, формирование политик безопасности компьютерных систем и сетей |
| *организационно-управленческий* | B/02.6 – Администрирование систем защиты информации автоматизированных систем  B/03.6 – Управление защитой информации в автоматизированных системах  В/06.6 - Аудит защищенности информации в автоматизированных системах  С/04.6 – Внедрение организационных мер по защите информации в автоматизированных системах  Е/01.8 - Обоснование необходимости защиты информации в автоматизированной системе;  Е/02.8 - Определение угроз безопасности информации, обрабатываемой автоматизированной системой  С/02.7 - Разработка требований по защите, формирование политик безопасности компьютерных систем и сетей |
| *эксплуатационный* | В/01.6 - Диагностика систем защиты информации автоматизированных систем  B/02.6 – Администрирование систем защиты информации автоматизированных систем  B/03.6 – Управление защитой информации в автоматизированных системах  В/04.6 - Обеспечение работоспособности систем защиты информации при возникновении нештатных ситуаций  В/05.6 - Мониторинг защищенности информации в автоматизированных системах  С/01.6 - Установка и настройка средств защиты информации в автоматизированных системах  Е/03.8 - Разработка архитектуры системы защиты информации автоматизированной системы  C/05.7 - Проведение инструментального мониторинга защищенности компьютерных систем и сетей  C/06.7 - Проведение экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов  C/03.6 - Документирование результатов реализации мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры |
| *проектно-технологический* | С/01.6 - Установка и настройка средств защиты информации в автоматизированных системах  С/03.6 - Анализ уязвимостей внедряемой системы защиты информации |
| *экспериментально-исследовательский* | С/01.6 - Установка и настройка средств защиты информации в автоматизированных системах |
| *научно-исследовательский* | E/04.8 - Моделирование защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации |
| *12 Обеспечение безопасности (в сфере обеспечения безопасности информации в автоматизированных системах, обладающих информационно-технологическими ресурсами, подлежащими защите)* | *проектный* | А/02.6 - Формирование мер по обеспечению безопасности значимых объектов значимых объектах критической информационной инфраструктуры объектов топливно-энергетического комплекса  А/03.6 - Разработка организационно-распорядительных документов по обеспечению безопасности значимых объектов значимых объектах критической информационной инфраструктуры объектов топливно-энергетического комплекса  D/02.7 - Разработка проектных решений по защите информации в автоматизированных системах;  D/03.7 - Разработка эксплуатационной документации на системы защиты информации автоматизированных систем.  D/02.8 - Проектирование программно-аппаратных средств защиты информации компьютерных систем и сетей;  С/02.7 - Разработка требований по защите, формирование политик безопасности компьютерных систем и сетей. |
| *контрольно-аналитический* | А/01.6 - Обоснование требований к системе безопасности значимых объектов на значимых объектах критической информационной инфраструктуры объектов топливно-энергетического комплекса  C/02.6 - Проведение контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации значимых объектов критической информационной инфраструктуры объектов топливно-энергетического комплекса.  D/01.7 - Выявление угроз безопасности информации значимых объектов критической информационной инфраструктуры критической информационной инфраструктуры объектов топливно-энергетического комплекса  D/02.7 - Организация и контроль функционирования системы безопасности и состояния безопасности значимых объектов критической информационной инфраструктуры, наличия в них уязвимостей  Е/02.8 - Определение угроз безопасности информации, обрабатываемой автоматизированной системой;  В/06.6 - Аудит защищенности информации в автоматизированных системах  D/04.8 - Сопровождение разработки средств защиты информации компьютерных систем и сетей.  В/01.6 - Диагностика систем защиты информации автоматизированных систем |
| *организационно-управленческий* | B/01.6 - Обеспечение реализации организационных мер и эксплуатации средств защиты информации значимых объектов критической информационной инфраструктуры объектов топливно-энергетического комплекса  Е/03.8 - Разработка архитектуры системы защиты информации автоматизированной системы.  D/04.8 - Сопровождение разработки средств защиты информации компьютерных систем и сетей.  В/03.6 - Управление защитой информации в автоматизированных системах  В/06.6 - Аудит защищенности информации в автоматизированных системах  С/02.6 - Разработка организационно-  распорядительных документов по защите информации в автоматизированных системах  С/04.6 - Внедрение организационных мер по защите информации в автоматизированных системах |
| *научно-исследовательский* | E/04.8 - Моделирование защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации |
| *эксплуатационный* | В/02.6 - Администрирование систем защиты информации автоматизированных систем  В/04.6 - Обеспечение работоспособности систем защиты информации при возникновении нештатных ситуаций  В/01.6 - Диагностика систем защиты информации автоматизированных систем  D/01.7 - Тестирование систем защиты информации автоматизированных систем  D/03.8 - Разработка и тестирование средств защиты информации компьютерных систем и сетей  В/05.6 - Мониторинг защищенности информации в автоматизированных системах |
| *проектно-технологический* | С/01.6 - Установка и настройка средств защиты информации в автоматизированных системах  С/03.6 - Анализ уязвимостей внедряемой системы защиты информации |
| *экспериментально-исследовательский* | С/01.6 - Установка и настройка средств защиты информации в автоматизированных системах |

# Раздел 3. ОБЩАЯ ХАРАКТЕРИСТИКА ОБРАЗОВАТЕЛЬНЫХ ПРОГРАММ, РЕАЛИЗУЕМЫХ В РАМКАХ НАПРАВЛЕНИЯ ПОДГОТОВКИ (СПЕЦИАЛЬНОСТИ) 10.05.03 «Информационная безопасность автоматизированных систем»

**3.1. Направленности (специализации) образовательных программ в рамках направления подготовки (специальности):**

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

специализация № 1 «Автоматизированные информационные системы специального назначения»;

специализация № 2 «Высокопроизводительные вычислительные системы специального назначения»;

специализация № 3 «Специальные технологии обеспечения информационной безопасности»;

специализация № 4 «Безопасность автоматизированных систем критически важных объектов»;

специализация № 5 «Безопасность открытых информационных систем»;

специализация № 6 «Безопасность автоматизированных систем в кредитно-финансовой сфере»;

специализация № 7 «Анализ безопасности информационных систем»;

специализация № 8 «Разработка автоматизированных систем в защищенном исполнении»;

специализация № 9 «Безопасность автоматизированных систем на транспорте» (по видам);

специализация № 10 «Безопасность автоматизированных систем управления технологическими процессами» (по отрасли или в сфере профессиональной деятельности);

специализация № 11 «Безопасность значимых объектов критической информационной инфраструктуры» (по отрасли или в сфере профессиональной деятельности).

Программы специалитета по специализациям № 1 «Автоматизированные информационные системы специального назначения», № 2 «Высокопроизводительные вычислительные системы специального назначения», № 3 «Специальные технологии обеспечения информационной безопасности» 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 зачетных единиц (далее – 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 ОВЗ 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. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий;

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

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

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

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

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

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

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 конфликтов;

УК-9. Способен принимать обоснованные экономические решения в различных областях жизнедеятельности

УК-10. Способен формировать нетерпимое отношение к коррупционному поведению

Перечень общепрофессиональных компетенций:

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-2. Способен применять программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности;

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

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

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

ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах 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 языках общего назначения, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ

ОПК-8. Способен применять методы научных исследований при проведении разработок в области защиты информации в автоматизированных системах

ОПК-9. Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации

ОПК-10. Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности

ОПК-11. Способен разрабатывать компоненты систем защиты информации автоматизированных систем

ОПК-12. Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем;

ОПК-13. Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем

ОПК-14. Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений

ОПК-15. Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем

ОПК-16. 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

Перечень общепрофессиональных компетенций по специализациям

специализация № 4 «Безопасность автоматизированных систем критически важных объектов»:

ОПК-4.1. Способен осуществлять внедрение и эксплуатацию систем защиты информации, использующихся на критически важных объектах и в автоматизированных системах критически важных объектов;

ОПК-4.2. Способен разрабатывать технические регламенты по обеспечению информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов;

ОПК-4.3. Способен разрабатывать системы защиты информации, функционирующие на критически важных объектах и в автоматизированных системах критически важных объектов;

специализация № 5 «Безопасность открытых информационных систем»:

ОПК-5.1. Способен разрабатывать и реализовывать политики информационной безопасности открытых информационных систем;

ОПК-5.2. Способен разрабатывать и эксплуатировать системы защиты информации открытых информационных систем;

ОПК-5.3. Способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах;

специализация № 6 «Безопасность автоматизированных систем в кредитно-финансовой сфере»:

ОПК-6.1. Способен организовать и обеспечить информационную безопасность при реализации технологических и бизнес-процессов организаций кредитно-финансовой сферы, в том числе процессов, связанных с осуществлением переводов денежных средств;

ОПК-6.2. Способен управлять инцидентами информационной безопасности, осуществлять контроль обеспечения информационной безопасности в организациях кредитно-финансовой сферы;

ОПК-6.3. Способен организовать защиту информации в автоматизированных системах, задействованных в реализации технологических и бизнес-процессов организаций кредитно-финансовой сферы, в соответствии с нормативными правовыми актами и нормативными методическими документами Банка России в области защиты информации;

специализация № 7 «Анализ безопасности информационных систем»:

ОПК-7.1. Способен использовать программные и программно-аппаратные средства для моделирования и испытания систем защиты информационных систем;

ОПК-7.2. Способен разрабатывать методики и тесты для анализа степени защищенности информационной системы и ее соответствия нормативным требованиям по защите информации;

ОПК-7.3. Способен проводить анализ защищенности и верификацию программного обеспечения информационных систем;

специализация № 8 «Разработка автоматизированных систем в защищенном исполнении»:

ОПК-8.1. Способен обосновать целесообразность создания автоматизированной системы в защищенном исполнении и формировать исходные требования к этой системе, процессу ее создания и эксплуатации;

ОПК-8.2. Способен организовать и осуществлять разработку проектных и организационных решений, документирование системы защиты информации автоматизированной системы в защищенном исполнении;

ОПК-8.3. Способен организовать и осуществлять обеспечение информационной безопасности процесса создания автоматизированной системы в защищенном исполнении;

специализация № 9 «Безопасность автоматизированных систем на транспорте» (по видам):

ОПК-9.1. Способен проектировать системы защиты информации автоматизированных, информационно-управляющих и информационно-логистических систем на транспорте (по видам) и сопровождать их разработку;

ОПК-9.2. Способен осуществлять внедрение и эксплуатацию систем защиты информации автоматизированных, информационно-управляющих и информационно-логистических систем на транспорте (по видам);

ОПК-9.3. Способен осуществлять контроль защищенности автоматизированных, информационно-управляющих и информационно-логистических систем на транспорте (по видам) с учетом установленных требований безопасности;

специализация № 10 «Безопасность автоматизированных систем управления технологическими процессами» (по отрасли или в сфере профессиональной деятельности):

ОПК-10.1. Способен планировать, разрабатывать и осуществлять мероприятия по обеспечению безопасности автоматизированных систем управления технологическими процессами;

ОПК-10.2. Способен проектировать системы защиты информации автоматизированных систем управления технологическими процессами с учетом установленных требований безопасности;

ОПК-10.3. Способен организовать и осуществлять контроль защищенности автоматизированных систем управления технологическими процессами;

специализация № 11 «Безопасность значимых объектов критической информационной инфраструктуры» (по отрасли или в сфере профессиональной деятельности):

ОПК-11.1. Способен планировать и разрабатывать меры по обеспечению безопасности значимых объектов критической информационной инфраструктуры;

ОПК-11.2. Способен обеспечить функционирование систем безопасности значимых объектов критической информационной инфраструктуры;

ОПК-11.3. Способен организовывать и осуществлять меры по контролю состояния безопасности значимых объектов критической информационной инфраструктуры.

Таблица 3

**Универсальные компетенции выпускников и индикаторы их достижения**

**специальность 10.05.03 Информационная безопасность автоматизированных систем**

| **Код и наименование ОПК** | **Код индикатора** | **Индикаторы достижения компетенций** | **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 ситуация 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 | Иностранпный 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-9. Способен принимать обоснованные экономические решения в различных областях жизнедеятельности** | УК-9.1.1 | знает основные виды доходов, финансовые инструменты, виды и источники возникновения экономических и финансовых рисков в экономике | Экономика |  |
| УК-9.1.2 | 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-9.1.3 | знает нормативные правовые акты, регламентирующие вопросы реализации бюджетно-налоговой и денежно-кредитной политики государства |
| УК-9.2.1 | 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-9.2.1 | умеет применять нормативные правовые акты при принятии экономических решений |
| **УК-10. Способен формировать нетерпимое отношение к коррупционному поведению** | УК-10.1.1 | знает содержание основных нормативных правовых актов в сфере противодействия коррупции | Дисциплина (модуль) части, формируемой участниками образовательных отношений |  |
| УК-10.2.2 | умеет соблюдать требования антикоррупционного законодательства, воздерживаться от поведения, вызывающего сомнение в объективном и беспристрастном исполнении должностных (служебных) обязанностей |

Таблица 4

**Общепрофессиональные компетенции выпускников и индикаторы их достижения**

**специальность 10.05.03 Информационная безопасность автоматизированных систем**

| **Код и наименование ОПК** | **Код** | **Индикаторы достижения общепрофессиональных компетенций** | **Наименование учебной, дисциплины (модуля), практики, НИР, ВКР, формирующие ОПК по примерному учебному плану** | **Код ПС, код ОТФ, ТФ, (при наличии)** |
| --- | --- | --- | --- | --- |
| 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 сущность и понятие информации, информационной безопасности и характеристику ее составляющих | Основы информационной безопасности | ПС 06.031  ОТФ-D  ТФ-D/01.7 |
| ОПК-1.1.2 | знает место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики |
| ОПК-1.1.3 | знает источники и классификацию угроз информационной безопасности |
| ОПК-1.1.4 | знает основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации |
| ОПК-1.1.5 | знает основные понятия, связанные с обеспечением информационной безопасности личности, общества и государства, понятия информационного противоборства, информационной войны и формы их проявлений в современном мире |
| ОПК-1.2.1 | умеет классифицировать и оценивать угрозы информационной безопасности. |
| ОПК-2. Способен применять программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности | ОПК-2.1.1 | знает общие принципы построения современных компьютеров, формы и способы представления данных в персональном компьютере | Информатика | ПС 06.001  ОТФ-А  ТФ-А/01.3 |
| ОПК-2.1.2 | знает логико-математические основы построения электронных цифровых устройств |
| ОПК-2.1.3 | знает состав, назначение аппаратных средств и программного обеспечения персонального компьютера |
| ОПК-2.2.1 | умеет применять типовые программные средства сервисного назначения, информационного поиска и обмена данными в сети Интернет |
| ОПК-2.2.2 | умеет составлять документы, используя прикладные программы офисного назначения |
| ОПК-2.2.3 | умеет пользоваться средствами пользовательских интерфейсов операционных систем |
| ОПК-3. Способен использовать математические методы, необходимые для решения задач профессиональной деятельности | ОПК-3.1.1 | знает основные понятия теории пределов и непрерывности функций одной и нескольких действительных переменных | Математический анализ | ПС 06.031  ОТФ-А  ТФ-А/01.7 |
| ОПК-3.1.2 | знает основные методы дифференциального исчисления функций одной и нескольких действительных переменных |
| ОПК-3.1.3 | знает основные методы интегрального исчисления функций одной и нескольких действительных переменных |
| ОПК-3.1.4 | знает основные методы исследования числовых и функциональных рядов |
| ОПК-3.1.5 | знает основные задачи теории функций комплексного переменного |
| ОПК-3.1.6 | знает основные типы обыкновенных дифференциальных уравнений и методы их решения |
| ОПК-3.2.1 | умеет исследовать функциональные зависимости, возникающие для решения стандартных прикладных задач |
| ОПК-3.2.2 | умеет использовать типовые модели и методы математического анализа для решения стандартных прикладных задач |
| ОПК-3.2.3 | умеет проводить типовые расчеты с использованием основных формул дифференциального и интегрального исчисления |
| ОПК-3.2.4 | умеет пользоваться справочными материалами по математическому анализу. |
| ОПК-3.1.7 | знает основные понятия теории вероятностей, числовые и функциональные характеристики распределений случайных величин и их основные свойства | Теория вероятностей и математическая статистика | ПС 06.031  ОТФ-E  ТФ-E/01.8 |
| ОПК-3.1.8 | знает классические предельные теоремы теории вероятностей |
| ОПК-3.1.9 | знает основные понятия теории случайных процессов |
| ОПК-3.1.10 | знает постановку задач и основные понятия математической статистики |
| ОПК-3.1.11 | знает стандартные ме­тоды получения точечных и интервальных оценок параметров вероятностных распределений |
| ОПК-3.1.12 | знает стандартные методы проверки статистических гипотез |
| ОПК-3.2.5 | умеет применять стандартные вероятностные и статистические мо­дели для решения типовых прикладных задач |
| ОПК-3.2.6 | умеет пользоваться стандартными вероятностно-статистическими методами анализа экс­пе­ри­мен­таль­ных дан­ных |
| ОПК-3.2.7 | умеет строить стандартные процедуры принятия решений на основе имеющихся экспериментальных данных |
| ОПК-3.2.8 | умеет использовать расчетные формулы и таблицы для решения стандартных вероятностно-статистических задач |
| ОПК-3.1.13 | знает основные понятия и задачи векторной алгебры и аналитической геометрии | Алгебра и геометрия | ПС 06.031  ОТФ-A  ТФ-A/03.7 |
| ОПК-3.1.14 | знает основные свойства алгебраических структур |
| ОПК-3.1.15 | знает основы линейной алгебры над произвольными полями |
| ОПК-3.2.9 | умеет строить и изучать математические модели конкретных явлений и процессов для решения расчетных и исследовательских задач |
| ОПК-3.2.10 | умеет решать основные задачи векторной алгебры и аналитической геометрии |
| ОПК-3.2.11 | умеет решать основные задачи линейной алгебры, системы линейных уравнений над полями |
| ОПК-3.2.12 | умеет использовать методы аналитической геометрии и векторной алгебры в смежных дисциплинах и физике |
| ОПК-3.2.13 | умеет использовать методы линейной алгебры для решения прикладных задач |
| ОПК-3.1.16 | знает свойства основных дискретных структур: конечных полей, графов, конечных автоматов, комбинаторных структур | Дискретная математика | ПС 06.031  ОТФ-A  ТФ-A/03.7 |
| ОПК-3.1.17 | знает основные понятия и методы теории графов |
| ОПК-3.1.18 | знает основные понятия и методы теории конечных автоматов |
| ОПК-3.1.19 | знает основные понятия и методы комбинаторного анализа |
| ОПК-3.2.14 | умеет решать задачи периодичности и эквивалентности для конечных автоматов |
| ОПК-3.2.15 | умеет применять аппарат производящих функций и рекуррентных соотношений для решения перечислительных задач |
| ОПК-3.2.16 | умеет решать оптимизационные задачи на графах |
| ОПК-3.2.17 | умеет применять стандартные методы дискретной математики для решения профессиональных задач |
| ОПК-3.2.18 | умеет решать типовые комбинаторные и теоретико-графовые задачи |
| ОПК-3.2.19 | умеет использовать язык и средства дискретной математики для решения профессиональных задач |
| ОПК-3.1.20 | знает основные понятия и определения теории информации | Теория информации (Теория информации и кодирования) | ПС 06.033  ОТФ-E  ТФ-E/04.8 |
| ОПК-3.2.20 | умеет определять информационные характеристики системы передачи сообщений и каналов связи |
| ОПК-3.1.21 | знает основные понятия математической логики, теории дискретных функций и теории алгоритмов, а также возможности применения общих логических принципов в математике и профессиональной деятельности | Математическая логика и теория алгоритмов |  |
| ОПК-3.1.22 | знает язык и средства современной математической логики и теории логических исчислений |
| ОПК-3.1.23 | знает основные способы задания булевых функций и функций многозначной логики формулами и их свойства |
| ОПК-3.1.24 | знает различные подходы к определению понятия алгоритма, методы доказательства алгоритмической неразрешимости и методы построения эффективных алгоритмов |
| ОПК-3.2.21 | умеет проводить основные логические операции в исчислении высказываний и исчислении предикатов |
| ОПК-3.2.22 | умеет находить и исследовать свойства представлений булевых и многозначных функций формулами в различных базисах |
| ОПК-3.2.23 | умеет оценивать сложность алгоритмов и вычислений |
| ОПК-3.2.24 | умеет упрощать формулы алгебры высказываний и алгебры предикатов |
| ОПК-3.2.25 | умеет применять методы и факты теории алгоритмов, относящиеся к решению переборных задач |
| ОПК-4. Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности | ОПК-4.1.1 | знает основные понятия, определения и принципы теории помехоустойчивого кодирования | Теория информации (Теория информации и кодирования) | ПС 06.033  ОТФ-E  ТФ-E/04.8 |
| ОПК-4.1.2 | знает основные способы кодирования информации |
| ОПК-4.2.1 | умеет применять |
| ОПК-4.1.3 | знает основные законы механики | Физика | ПС 06.033 ОТФ–E  ТФ-E/04.8 |
| ОПК-4.1.4 | знает основные положения термодинамики и молекулярной физики |
| ОПК-4.1.5 | знает основные законы электричества и магнетизма |
| ОПК-4.1.6 | знает основные законы теории колебаний и волн, волновой оптики |
| ОПК-4.1.7 | знает основные принципы квантовой физики. |
| ОПК-4.2.2 | умеет проводить физический эксперимент, обрабатывать его результаты и делать выводы о проделанной исследовательской работе |
| ОПК-4.2.3 | умеет решать типовые прикладные физические задачи |
| ОПК-4.2.4 | уметь работать с современной измерительной техникой. |
| ОПК-4.1.8 | знает основополагающие принципы работы элементов и функциональных узлов электронной аппаратуры. | Электроника и схемотехника |  |
| ОПК-4.2.5 | умеет анализировать компонентную базу электронной аппаратуры. |
| ОПК-4.1.9 | знает терминологию, основные руководящие и регламентирующие документы в области ЭВМ и вычислительных систем | Организация ЭВМ и вычислительных систем (Аппаратные средства вычислительной техники) | ПС 06.032  ОТФ-A  ТФ-А/3.5 |
| ОПК-4.2.6 | умеет осуществлять сбор, обработку, анализ и систематизацию научно-технической информации в области ЭВМ и систем с применением современных информационных технологий |
| ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации | ОПК-5.1.1 | знает основы: российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации | Организационное и правовое обеспечение информационной безопасности | ПС 06.033  ОТФ – D  ТФ–D/03.7 |
| ОПК-5.1.2 | знает основные понятия и характеристику основных отраслей права, применяемых в профессиональной деятельности организации |
| ОПК-5.1.3 | знает основы законодательства Российской Федерации, нормативные правовые акты, нормативные и методические документы в области информационной безопасности и защиты информации, правовые основы организации защиты государственной тайны и конфиденциальной информации, правовую характеристику преступлений в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за разглашение защищаемой информации |
| ОПК-5.1.4 | знает правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности |
| ОПК-5.2.1 | умеет обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав |
| ОПК-5.2.2 | умеет анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации |
| ОПК-5.2.3 | умеет формулировать основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации |
| ОПК-5.2.4 | умеет формулировать основные требования информационной безопасности при эксплуатации автоматизированной системы |
| ОПК-5.2.5 | умеет формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации |
| ОПК-5.1.5 | знает основы: российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации |
| ОПК-5.1.6 | знает нормативные документы в области технической защиты информации | Защита информации от утечки по техническим каналам | ПС 06.033  ОТФ-E  ТФ-E/04.8 |
| ОПК-5.1.7 | знает основные документы по стандартизации в сфере управления ИБ | Управление информационной безопасностью | ПС 06.033  ОТФ – D  ТФ–D/03.7 |
| ОПК-5.1.8 | знает принципы формирования политики информационной безопасности в автоматизированных системах |
| ОПК-5.1.9 | знает требования информационной безопасности при эксплуатации автоматизированной системы |
| ОПК-5.2.6 | умеет формировать политики информационной безопасности организации |
| ОПК-5.2.7 | умеет выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы |
| ОПК-5.1.10 | знает условные графические обозначения видов проводки, материалов конструкций, электронных компонентов в соответствии с требованиями ЕСПД и ЕСКД | Инженерная и компьютерная графика (Инженерная графика) | ПС 06.033  ОТФ-D  ТФ-D/04.7 |
| ОПК-5.2.8 | умеет использовать программные средства для построения графических схем и алгоритмов в соответствии с требованиями ЕСПД и ЕСКД |
| ОПК-6. Способен при решении профессиональных задач организовать защиту информации ограниченного доступа в автоматизированных системах 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 систему нормативных правовых актов и стандартов по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации | Организационное и правовое обеспечение информационной безопасности | ПС 06.034  ОТФ –I  ТФ –I/01.8,  ПС 06.031  ОТФ-D  ТФ-D/01.7 |
| ОПК-6.1.2 | знает задачи органов защиты государственной тайны и служб защиты информации на предприятиях |
| ОПК-6.1.3 | знает систему организационных мер, направленных на защиту информации ограниченного доступа |
| ОПК-6.1.4 | знает нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа | Защита информации от утечки по техническим каналам | ПС 06.034 ОТФ – G ТФ-G/01.7  ПС 06.034 ОТФ-G ТФ-G/01.7 |
| ОПК-6.1.5 | знает основные угрозы безопасности информации и модели нарушителя объекта информатизации |
| ОПК-6.2.1 | умеет разрабатывать модели угроз и модели нарушителя объекта информатизации |
| ОПК-6.2.2 | умеет разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации |
| ОПК-6.2.3 | умеет определить политику контроля доступа работников к информации ограниченного доступа |
| ОПК-6.2.4 | умеет формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации |
| ОПК-7. Способен создавать программы на языках общего назначения, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ | ОПК-7.1.1 | знает общие принципы построения, области и особенности применения языков программирования высокого уровня | Языки программирования | ПС 06.001 ОТФ–D ТФ-D/03.6,  ПС 06.001 ОТФ – A ТФ-A/02.3,  ПС 06.001 ОТФ–A  ТФ-A/01.3,  ПС 06.001 ОТФ – A ТФ-A/02.3,  ПС 06.001 ОТФ – A ТФ-A/02.3 |
| ОПК-7.1.2 | знает язык программирования высокого уровня (объектно-ориентированное программирование) |
| ОПК-7.2.1 | умеет работать с интегрированной средой разработки программного обеспечения |
| ОПК-7.2.2 | умеет разрабатывать и реализовывать на языке высокого уровня алгоритмы решения типовых профессиональных задач |
| ОПК-7.1.3 | знает современные технологии и методы программирования | Технологии и методы программирования | ПС 06.001 ОТФ-A ТФ-A/01.3 |
| ОПК-7.1.4 | знает принципы организации документирования разработки, процесса сопровождения программного обеспечения |
| ОПК-7.2.3 | умеет проектировать структуру и архитектуру программного обеспечения с использованием современных методологий и средств автоматизации проектирования программного обеспечения |
| ОПК-7.1.5 | знает показатели качества программного обеспечения |
| ОПК-7.2.4 | умеет применять известные методы программирования и возможности базового языка программирования для решения типовых профессиональных задач |
| ОПК-7.1.6 | знает основные алгоритмы сортировки и поиска данных, комбинаторные и теоретико-графовые алгоритмы |
| ОПК-8. Способен применять методы научных исследований при проведении разработок в области защиты информации в автоматизированных системах | ОПК-8.1.1 | знает методологические основы научных исследований | Основы научных исследований |  |
| ОПК-8.2.1 | умеет работать с научной, научно-технической и патентной литературой |
| ОПК-8.2.2 | умеет обрабатывать результаты научных исследований |
| ОПК-8.1.2 | знает порядок подготовки, выполнения и защиты квалификационных и иных научных работ (курсовые и дипломные работы, отчеты о НИР, диссертации и др.) |
| ОПК-9. Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации | ОПК-9.1.1 | знает основные характеристики сигналов электросвязи, спектры и виды модуляции | Сети и системы передачи информации | ПС 06.032  ОТФ-В  ТФ-B/02.6,  ПС 06.033  ОТФ-E  ТФ-E/04.8 |
| ОПК-9.1.2 | знает способы кодирования информации |
| ОПК-9.2.1 | умеет анализировать основные характеристики и возможности телекоммуникационных систем |
| ОПК-9.1.3 | знает текущее состояние и тенденции развития методов и средств защиты информации в операционных системах, съемных носителях и сетях передачи данных | Программно-аппаратные средства защиты информации | ПС 06.033  ОТФ-B  ТФ-В/03.6,  ПС 06.11  ОТФ-C  ТФ-C/15.5,  ПС 06.032  ОТФ-С  ТФ-C/05.7 |
| ОПК-9.1.4 | знает принципы построения и особенности функционирования систем контроля и управления доступом в автоматизированных системах; |
| ОПК-9.1.5 | знает подходы к анализу защищенности компонентов автоматизированных систем и поиску потенциальных уязвимостей безопасности информации |
| ОПК-9.2.2 | умеет анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах |
| ОПК-10. Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности | ОПК-10.1.1 | знает принципы организации и структуру систем защиты информации современных операционных систем | Безопасность операционных систем | ПС 06.033 ОТФ – D ТФ-D/01.7 |
| ОПК-10.1.2 | знает критерии оценки эффективности и надежности систем защиты информации операционных систем |
| ОПК-10.2.1 | умеет конфигурировать параметры системы защиты информации современных операционных систем |
| ОПК-10.2.2 | умеет контролировать эффективность принятых мер по реализации политик безопасности информации в современных операционных системах |
| ОПК-10.2.3 | умеет проводить анализ угроз безопасности в локальных вычислительных сетях | Безопасность вычислительных сетей | ПС 06.030 ОТФ-Е ТФ-Е/01.7 |
| ОПК-10.1.3 | знает основные протоколы, используемые для защиты информации в вычислительных сетях |
| ОПК-10.1.4 | знает основные криптографические методы, используемые для защиты информации в вычислительных сетях |
| ОПК-10.1.5 | знает основные задачи и понятия криптографии | Методы и средства криптографической защиты информации | ПС 06.030 ОТФ – А ТФ-А/02.5,  ПС 06.030 ОТФ – С ТФ-С/02.6 |
| ОПК-10.1.6 | знает модели шифров и математические методы их исследования |
| ОПК-10.2.4 | умеет применять математические методы исследования моделей шифров |
| ОПК-10.2.5 | умеет использовать типовые криптографические алгоритмы |
| ОПК-11. Способен разрабатывать компоненты систем защиты информации автоматизированных систем | ОПК-11.1.1 | знает методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем | Разработка и эксплуатация автоматизированных систем в защищенном исполнении | ПС 06.033 ОТФ-D ТФ-D/02.7,  ПС 06.033 ОТФ–D ТФ–D/01.7,  ПС 06.033 ОТФ-D ТФ-D/02.7 |
| ОПК-11.1.2 | знает методы, способы, средства, последовательность и содержание этапов разработки систем защиты информационной автоматизированных систем |
| ОПК-11.1.3 | знает методы, способы и средства обеспечения отказоустойчивости автоматизированных систем |
| ОПК-11.2.1 | умеет проектировать защищенные автоматизированные системы с учетом действующих нормативных и методических документов |
| ОПК-11.2.2 | умеет разрабатывать техническую документацию на компоненты автоматизированных систем |
| ОПК-12. Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем | ОПК-12.1.1 | знает принципы построения и функционирования, примеры реализаций современных операционных систем | Безопасность операционных систем | ПС 06.033 ОТФ – D ТФ-D/01.7 |
| ОПК-12.2.1 | умеет оценивать эффективность и надежность защиты операционных систем |
| ОПК-12.1.2 | знает принципы построения и функционирования локальных и глобальных вычислительных сетей | Безопасность вычислительных сетей | ПС 06.030 ОТФ-Е ТФ-Е/01.7 |
| ОПК-12.1.3 | знает последовательность и содержание этапов построения локальных вычислительных сетей |
| ОПК-12.1.4 | знает принципы построения и функционирования, примеры реализаций современных систем управления базами данных | Безопасность систем баз данных | ПС 06.011 ОТФ–E ТФ-E/01.7 |
| ОПК-12.2.2 | умеет разрабатывать и администрировать базы данных |
| ОПК-13. Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем | ОПК-13.1.1 | знает технические характеристики, основные показатели качества и эффективности ЭВМ и вычислительных систем, методы их оценки и пути совершенствования | Организация ЭВМ и вычислительных систем (Аппаратные средства вычислительной техники) |  |
| ОПК-13.2.1 | умеет проводить анализ архитектуры и структуры ЭВМ и вычислительных систем |
| ОПК-13.2.2 | умеет проводить тестирование и отладку программных систем | Технологии и методы программирования | ПС 06.001 ОТФ-B ТФ-B/02.4 |
| ОПК-13.1.2 | знает методы тестирования и отладки программного обеспечения |
| ОПК-13.1.3 | знает способы и средства контроля эффективности защиты информации | Защита информации от утечки по техническим каналам | ПС 06.033 ОТФ-D ТФ-D/03.7 |
| ОПК-13.1.4 | знает способы и средства защиты информации от утечки по техническим каналам |
| ОПК-13.1.5 | знает технические каналы утечки информации |
| ОПК-13.2.3 | умеет использовать средства инструментального контроля показателей эффективности технической защиты информации |
| ОПК-13.1.6 | знает основные угрозы безопасности информации и модели нарушителя в автоматизированных системах | Разработка и эксплуатация автоматизированных систем в защищенном исполнении | ПС 06.033 ОТФ – А ТФ-А/01.5,  ПС 06.034 ОТФ-F ТФ-F/02.7 |
| ОПК-13.1.7 | знает содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации |
| ОПК-13.2.4 | умеет осуществлять контроль обеспечения уровня защищенности в автоматизированных системах |
| ОПК-13.2.5 | умеет обнаруживать и устранять нарушения правил разграничения доступа в автоматизированных системах |
| ОПК-13.2.6 | умеет определять источники и причины возникновения инцидентов безопасности в автоматизированных системах |
| ОПК-13.2.7 | умеет контролировать события безопасности и действия пользователей автоматизированных систем |
| ОПК-13.2.8 | умеет контролировать эффективность принятых мер по реализации политик безопасности информации автоматизированных систем |
| ОПК-13.2.9 | умеет документировать процедуры и результаты контроля функционирования системы защиты информации автоматизированной системы |
| ОПК-14. Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений | ОПК-14.1.1 | знает основные угрозы безопасности информации и модели нарушителя в автоматизированных системах | Организационное и правовое обеспечение информационной безопасности |  |
| ОПК-14.1.2 | знает критерии оценки эффективности и надежности средств защиты информации программного обеспечения автоматизированных систем | Разработка и эксплуатация автоматизированных систем в защищенном исполнении | ПС 06.033 ОТФ – А ТФ-А/01.5,  ПС 06.034 ОТФ-F ТФ-F/02.7 |
| ОПК-14.2.1 | умеет осуществлять планирование и организацию работы персонала автоматизированной системы с учетом требований по защите информации |
| ОПК-14.2.2 | умеет определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем |
| ОПК-15. Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем | ОПК-15.1.1 | знает принципы организации и структуру систем защиты информации современных операционных систем | Безопасность операционных систем | ПС 06.032 ОТФ-В ТФ-В/01.6 |
| ОПК-15.2.1 | умеет проводить установку и настройку современных операционных систем с учетом требований по обеспечению информационной безопасности |
| ОПК-15.2.2 | умеет использовать средства операционных систем для обеспечения безопасного функционирования автоматизированных систем |
| ОПК-15.2.3 | умеет восстанавливать операционные системы после сбоев |
| ОПК-15.2.4 | умеет реализовывать политику безопасности в локальной вычислительной сети | Безопасность вычислительных сетей | ПС 06.030 ОТФ–D ТФ-D/01.7 |
| ОПК-15.1.2 | знает средства защиты информации систем управления базами данных | Безопасность систем баз данных | ПС 06.032  ОТФ-В  ТФ-В/02.6 |
| ОПК-15.2.5 | умеет конфигурировать средства защиты информации систем управления базами данных |
| ОПК-15.1.3 | знает программные средства, позволяющие вести автоматизированный аудит | Управление информационной безопасностью | ПС 06.033 ОТФ-D ТФ-D/01.7,  ПС 06.034 ОТФ – D ТФ-D/01.6; D/02.6; D/03.6; |
| ОПК-15.2.6 | умеет осуществлять выбор и обоснование критериев эффективности функционирования защищенных автоматизированных информационных систем |
| ОПК-15.2.7 | умеет разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы |
| ОПК-16. 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-16.1.1 | знает периодизацию, основные факты, явления и процессы всемирной и отечественной истории | История (История России, Всеобщая история) |  |
| ОПК-16.1.2 | знает особенности исторического пути России, ее место и роль в мировом сообществе в контексте всеобщей истории |
| ОПК-16.2.1 | умеет анализировать основные этапы и закономерности исторического развития России, в том числе для формирования гражданской позиции и развития патриотизма |
| ОПК-4.1. Способен осуществлять внедрение и эксплуатацию систем защиты информации, использующихся на критически важных объектах и в автоматизированных системах критически важных объектов | ОПК-4.1.1.1 | знает порядок разработки технических регламентов для проведения аттестации объектов информатизации по требованиям безопасности информации на критически важных объектах | Информационная безопасность автоматизированных систем критически важных объектов | ПС 06.007- ОТФ А, ТФ A/01.6; ПС 06.018- ОТФ D, ТФ D/03.7 |
| ОПК-4.1.1.2 | знает нормативно-методическую базу, регламентирующую деятельность критически важных объектов и обеспечение их информационной безопасности |
| ОПК-4.1.2.1 | умеет применять нормативную базу, регламентирующую деятельность критически важных объектов и обеспечение их информационной безопасности |
| ОПК-4.1.2.2 | умеет разрабатывать технические регламенты для проведения аттестации объектов информатизации по требованиям безопасности информации на критически важных объектах |
| ОПК-4.1.3.1 | владеет методиками разработки технических регламентов для испытаний объектов информатизации на соответствие требованиям по защите информации автоматизированных систем критически важных объектов |
| ОПК-4.1.3.2 | владеет навыками настройки средств обеспечения информационной безопасности автоматизированных систем критически важных объектов |
| ОПК-4.2. Способен разрабатывать технические регламенты по обеспечению информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов | ОПК-4.2.1.1 | знает методы проведения технических регламентов по обеспечению информационной безопасности критически важных объектов и их автоматизированных систем | Мониторинг информационной безопасности критически важных объектов | ПС 06.007- ОТФ А, ТФ A/01.6; ПС 06.018- ОТФ D, ТФ D/03.7 |
| ОПК-4.2.2.1 | умеет вести мониторинг информационной безопасности критически важных объектов |
| ОПК-4.3. Способен разрабатывать системы защиты информации, функционирующие на критически важных объектах и в автоматизированных системах критически важных объектов | ОПК-4.3.1.1 | знает методы измерения частотных и временных параметров сигнальных демаскирующих признаков объектов мониторинга | Мониторинг информационной безопасности критически важных объектов | ПС 06.007- ОТФ А, ТФ A/01.6; ПС 06.018- ОТФ D, ТФ D/03.7 |
| ОПК-4.3.1.2 | знает алгоритмы измерения несущей частоты сигнала и частоты его побочных и внеполосных излучений |
| ОПК-4.3.1.3 | знает алгоритмы измерения ширины спектра сигнала |
| ОПК-4.3.1.4 | знает законы изменения или модуляции несущей частоты сигнала |
| ОПК-4.3.1.5 | знает порядок определения количества излучаемых фиксированных частот и величины разноса между ними |
| ОПК-4.3.2.1 | умеет проводить измерения частотных параметров сигнальных демаскирующих признаков объектов мониторинга |
| ОПК-4.3.2.2 | умеет применять современные средства и комплексы радио и радиотехнического контроля для измерения частотных параметров сигналов |
| ОПК-4.3.1.6 | знает методы измерения частотных и временных параметров сигнальных демаскирующих признаков объектов мониторинга | Основы построения средств и комплексов обеспечения информационной безопасности | ПС 06.007- ОТФ А, ТФ A/01.6; ПС 06.018- ОТФ D, ТФ D/03.7 |
| ОПК-4.3.1.7 | знает алгоритмы измерения несущей частоты сигнала и частоты его побочных и внеполосных излучений |
| ОПК-4.3.1.8 | знает алгоритмы измерения ширины спектра сигнала |
| ОПК-4.3.1.9 | знает законы изменения или модуляции несущей частоты сигнала |
| ОПК-4.3.1.10 | знает порядок определения количества излучаемых фиксированных частот и величины разноса между ними |
| ОПК-4.3.2.1 | умеет проводить измерения частотных параметров сигнальных демаскирующих признаков объектов мониторинга; |
| ОПК-4.3.2.2 | умеет применять современные средства и комплексы радио и радиотехнического контроля для измерения частотных параметров сигналов. |
| ОПК-5.1. Способен разрабатывать и реализовывать политику информационной безопасности открытых информационных систем | ОПК-5.1.1.1. | знает основные криптографические протоколы и стандарты; | Криптографические протоколы и стандарты | ПС 06.033- ОТФ В, ТФ В/03.6; |
| ОПК-5.1.1.2 | знает критерии оценки и контроля эффективности используемых криптографических протоколов и стандартов; |
| ОПК-5.1.2.1 | умеет выбирать криптографические протоколы и стандарты, для обеспечения информационной безопасности открытых информационных систем; |
| ОПК-5.1.2.2 | умеет осуществлять контроль эффективности средств защиты, реализующих используемые криптографические протоколы и стандарты; |
| ОПК-5.2. Способен разрабатывать и эксплуатировать системы защиты информации открытых информационных систем | ОПК-5.2.1.1 | знает методы и средства обеспечения информационной безопасности открытых информационных систем; | Информационная безопасность открытых систем | ПС 06.033 ОТФ В, ТФ В/04.6 |
| ОПК-5.2.1.2 | знает методы контроля, разработки эксплуатационной документации, обслуживания систем защиты информации открытых информационных систем; |
| ОПК-5.2.2.1 | умеет применять методы и средства защиты информации открытых информационных систем; |
| ОПК-5.2.2.2 | умеет разрабатывать эксплуатационную документацию, требования по эксплуатации систем защиты открытых информационных систем; |
| ОПК-5.3. Способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах | ОПК-5.3.1.1 | знает основные информационные технологии, используемые в автоматизированных системах; | Открытые информационные системы | ПС 06.033 ОТФ Е, ТФ Е/03.8 |
| ОПК-5.3.1.2 | знает системы управления информационной безопасностью открытой информационной системы; |
| ОПК-5.3.2.1 | умеет работать с интегрированной средой разработки программного обеспечения; |
| ОПК-5.3.2.2 | умеет анализировать представленную в общедоступных источниках информацию о современных тенденциях в области информационных систем; |
| ОПК-6.1. Способен организовывать и обеспечивать информационную безопасность при реализации технологических и бизнес-процессов организаций кредитно-финансовой сферы, в том числе процессов, связанных с осуществлением переводов денежных средств | ОПК-6.1.1.1 | знает подлежащие защите типовые технологические и бизнес-процессы организаций кредитно-финансовой сферы, в том числе связанные с осуществлением переводов денежных средств | Платежные системы и их безопасность | ПС 06.033 ОТФ B ТФ B/02.6 |
| ОПК-6.1.1.2 | знает основные угрозы безопасности информации при осуществлении переводов денежных средств с использованием платежных систем, пластиковых карт, систем дистанционного банковского обслуживания и др. |
| ОПК-6.1.1.3 | знает принципы формирования политики информационной безопасности в организациях кредитно-финансовой сферы |
| ОПК-6.1.2.1 | умеет регистрировать события, связанные с защитой информации при реализации технологических и бизнес-процессов организаций кредитно-финансовой сферы, в том числе при осуществлении переводов денежных средств |
| ОПК-6.2. Способен управлять инцидентами информационной безопасности, осуществлять контроль обеспечения информационной безопасности в организациях кредитно-финансовой сферы | ОПК-6.2.1.1 | знает принципы выявления, учета и устранения инцидентов, возникающих в автоматизированных системах организаций кредитно-финансовой сферы | Управление инцидентами и непрерывностью бизнеса в организациях финансово-кредитной сферы | ПС 06.033 ОТФ B ТФ B/01.6 ТФ B/04.6 |
| ОПК-6.2.1.2 | знает методы и способы обеспечения отказоустойчивости автоматизированных систем организаций кредитно-финансовой сферы |
| ОПК-6.2.2.1 | умеет обнаруживать и устранять инциденты информационной безопасности, возникающие в процессе эксплуатации автоматизированных систем организаций кредитно-финансовой сферы |
| ОПК-6.3. Способен организовывать защиту информации в автоматизированных системах, задействованных в реализации технологических и бизнес-процессов организаций кредитно-финансовой сферы, в соответствии с нормативными правовыми актами и нормативными методическими документами Банка России в области защиты информации | ОПК-6.3.1.4 | знает стандарты в области обеспечения информационной безопасности организаций кредитно-финансовой сферы | Нормативная база обеспечения информационной безопасности организаций финансово-кредитной сферы | ПС 06.033 ОТФ B ТФ B/01.6 ТФ B/02.6 ТФ B/03.6 ОТФ D ТФ D/02.7 |
| ОПК-6.3.1.5 | знает требования к обеспечению информационной безопасности организаций кредитно-финансовой сферы |
| ОПК-6.3.1.6 | знает критерии оценки информационной безопасности организаций кредитно-финансовой сферы |
| ОПК-6.3.1.7 | знает требования к управлению риском нарушения информационной безопасности при аутсорсинге существенных функций |
| ОПК-6.3.2.5 | умеет определять уровень обеспечения информационной безопасности организаций кредитно-финансовой сферы |
| ОПК-6.3.2.6 | умеет оценивать риск нарушения информационной безопасности при аутсорсинге существенных функций |
| ОПК-6.3.3.1 | владеет методикой оценки соответствия информационной безопасности организаций кредитно-финансовой сферы требованиям отраслевых стандартов |
| ОПК-6.3.1.1 | знает основные угрозы безопасности информации и модели нарушителя в автоматизированных системах организаций финансово-кредитной сферы | Защита информации в автоматизированных системах организаций финансово-кредитной сферы | ПС 06.033 ОТФ B ТФ B/01.6 ТФ B/02.6 ТФ B/03.6 ОТФ D ТФ D/02.7 |
| ОПК-6.3.1.2 | знает программно-аппаратные средства защиты информации автоматизированных систем организаций кредитно-финансовой сферы |
| ОПК-6.3.1.3 | знает криптографические средства и протоколы, используемые для защиты информации в автоматизированных системах организаций кредитно-финансовой сферы |
| ОПК-6.3.2.1 | умеет определять подлежащие защите информационные ресурсы автоматизированных систем организаций кредитно-финансовой сферы |
| ОПК-6.3.2.2 | умеет обеспечивать безопасность информации с учетом требований политики информационной безопасности в организациях кредитно-финансовой сферы |
| ОПК-6.3.2.3 | умеет составлять комплекс правил, процедур и средств обеспечения информационной безопасности автоматизированных систем организаций кредитно-финансовой сферы |
| ОПК-6.3.2.4 | умеет определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем в кредитно-финансовой сфере |
| ОПК-7.1. Способен использовать программные и программно-аппаратные средства для моделирования и испытания систем защиты информационных систем | ОПК-7.1.1.1 | знает технические средства контроля эффективности мер защиты информации | Анализ безопасности информационных систем | ПС 06.033 ОТФ-D ТФ-D/02.7 |
| ОПК-7.1.1.2 | знает принципы организации и структуру систем защиты информации программного обеспечения автоматизированных систем |
| ОПК-7.1.1.3 | знает программно-аппаратные средства обеспечения защиты информации автоматизированных систем |
| ОПК-7.1.2.2 | умеет выбирать меры защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы |
| ОПК-7.1.3.1 | владеет навыками использования программно-аппаратных средств обеспечения безопасности информации в автоматизированных системах |
| ОПК-7.2. Способен разрабатывать методики и тесты для анализа степени защищенности информационной системы и ее соответствия нормативным требованиям по защите информации | ОПК-7.2.1.1 | знает основные меры по защите информации в автоматизированных системах | Верификация безопасности информационных систем | ПС 06.033 ОТФ-D ТФ-D/03.7 |
| ОПК-7.2.1.2 | знает принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем |
| ОПК-7.2.1.3 | знает программно-аппаратные средства обеспечения защиты информации в программном обеспечении автоматизированных систем |
| ОПК-7.2.2.1 | умеет контролировать безотказное функционирование технических средств защиты информации |
| ОПК-7.2.2.2 | умеет определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем |
| ОПК-7.2.2.3 | умеет проводить технико-экономическое обоснование проектных решений программно-аппаратных средств обеспечения защиты информации в автоматизированной системе с целью обеспечения требуемого уровня защищенности |
| ОПК-7.2.3.1 | владеет методами выявления уязвимости информационно-технологических ресурсов автоматизированных систем |
| ОПК-7.2.1.4 | знает специфику конструктивного исполнения антенно-фидерных устройств |
| ОПК-7.2.1.5 | знает основные тенденции развития теории и техники антенн и сверхвысокочастотных устройств |
| ОПК-7.2.1.6 | знает методы расчета и измерения основных параметров линий передачи сверхвысокочастотного диапазона |
| ОПК-7.2.2.4 | умеет производить измерение основных характеристик и параметров элементов антенно-фидерных устройств |
| ОПК-7.2.3.2 | владеет методами расчета и измерения основных параметров устройств СВЧ, антенн и линий передачи сверхвысокочастотного диапазона |
| ОПК-7.3. Способен проводить анализ защищенности и верификацию программного обеспечения информационных систем | ОПК-7.3.1.1 | знает национальные, межгосударственные и международные стандарты в области защиты информации | *Анализ рисков информационной безопасности* | ПС 06.033 ОТФ-Е ТФ- Е/01.8 ОТФ-В ТФ- В/06.6 |
| ОПК-7.3.1.2 | знает последствия от нарушения свойств безопасности информации |
| ОПК-7.3.1.3 | знает основные угрозы безопасности информации и модели нарушителя в автоматизированных системах |
| ОПК-7.3.2.1 | умеет анализировать цели создания автоматизированных систем и задачи, решаемые автоматизированными системами |
| ОПК-7.3.2.2 | умеет оценивать информационные риски в автоматизированных системах |
| ОПК-8.1. Способен обосновывать целесообразность создания автоматизированной систем в защищенном исполнении и формировать исходные требования к этой системе, процессу ее создания и эксплуатации | ОПК-8.1.1.1 | знает порядок установки и настройки сертифицированных операционных систем | Администрирование автоматизированных систем в защищенном исполнении |  |
| ОПК-8.1.1.2 | знает порядок установки, настройки и обновления сертифицированного программного обеспечения и технических средств защиты информации |
| ОПК-8.1.1.3 | знает порядок проведения аудита защищенности автоматизированной системы |
| ОПК-8.1.2.1 | умеет обосновывать целесообразность создания автоматизированной систем в защищенном исполнении |
| ОПК-8.1.2.2 | умеет формировать исходные требования к автоматизированной систем в защищенном исполнении, процессу ее создания и эксплуатации |
| ОПК-8.2. Способен обеспечивать и осуществлять разработку проектных и организационных решений, документирование системы защиты информации автоматизированной системы в защищенном исполнении | ОПК-8.2.1.1 | знает базовые принципы и задачи проектной деятельности | Организация проектной деятельности |  |
| ОПК-8.2.1.2 | знает содержание и этапы проектной десятельности по созданию автоматизированных систем в защищенном исполнении |
| ОПК-8.2.1.3 | знает методы и инструменты проведения исследований в ходе проектной деятельности |
| ОПК-8.2.2.1 | умеет обеспечивать и осуществлять разработку проектных и организационных решений |
| ОПК-8.2.2.2 | умеет анализировать и составлять нормативные методические документы по обеспечению информационной безопасности программно-аппаратными средствами |
| ОПК-8.3. Способен организовывать и обеспечивать информационную безопасность процесса создания автоматизированной системы в защищенном исполнении | ОПК-8.3.1.1 | знает содержание и порядок выполнения работ на стадиях и этапах создания автоматизированных систем в защищенном исполнении | Информационная безопасность автоматизированных систем в защищенном исполнении |  |
| ОПК-8.3.1.2 | знает содержание и порядок выполнения работ по защите информации о создаваемой автоматизированной системе в защищенном исполнении |
| ОПК-8.3.1.3 | знает порядок установки, монтажа, настройки и технического обслуживания технических средств защиты информации в соответствии с требованиями эксплуатационной документации |
| ОПК-8.3.1.4 | знает порядок измерения параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа |
| ОПК-8.3.1.5 | знает порядок измерения параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации |
| ОПК-8.3.2.1 | умеет проводить тестирование функций отдельных программных и программно-аппаратных средств защиты информации |
| ОПК-9.1. Способен проектировать системы защиты информации автоматизированных, информационно-управляющих и информационно-логистических систем на транспорте (по видам) и сопровождать их разработку | ОПК-9.1.1.1 | знает особенности проектирования систем защиты информации автоматизированных систем на транспорте | Информационная безопасность автоматизированных систем на транспорте | ПС 06.033- ОТФ D |
| ОПК-9.1.2.1 | умеет проектировать систему защиты информации автоматизированных систем на транспорте |
| ОПК-9.1.3.1 | владеет навыками применения методов и средств защиты информации при построении систем защиты информации автоматизированных систем на транспорте |
| ОПК-9.1.1.2 | знает особенности проектирования систем защиты информации информационно-управляющих и информационно-логистических систем на транспорте | Информационная безопасность информационно-управляющих и информационно-логистических систем на транспорте |
| ОПК-9.1.2.2 | умеет проектировать систему защиты информации информационно-управляющих и информационно-логистических систем на транспорте, в том числе автоматизированных систем управления технологическими процессами |
| ОПК-9.1.3.2 | владеет навыками применения методов и средств защиты информации при построении систем защиты информации информационно-управляющих и информационно-логистических систем на транспорте, в том числе автоматизированных систем управления технологическими процессами |
| ОПК-9.1.1.3 | знает особенности анализа безопасности программного обеспечения при разработке систем защиты информации автоматизированных систем на транспорте | Анализ безопасности программного обеспечения автоматизированных систем на транспорте |
| ОПК-9.1.2.3 | умеет проводить анализ безопасности программного обеспечения при разработке систем защиты информации автоматизированных систем на транспорте |
| ОПК-9.1.3.3 | владеет навыками применения инструментальных средств анализа безопасности программного обеспечения при построении систем защиты информации автоматизированных систем на транспорте |
| ОПК-9.1.1.4 | знает особенности проектирования систем защиты информации корпоративных сетей передачи данных (по видам транспорта) | Технология защиты в корпоративных сетях передачи данных (по видам транспорта) | ПС 06.033- ОТФ D |
| ОПК-9.1.2.4 | умеет проектировать систему защиты информации корпоративных сетей передачи данных (по видам транспорта) |
| ОПК-9.1.3.4 | владеет навыками применения методов и средств защиты информации при построении систем защиты информации корпоративных сетей передачи данных (по видам транспорта) |
| ОПК-9.2. Способен осуществлять внедрение и эксплуатацию систем защиты информации автоматизированных, информационно-управляющих и информационно-логистических систем на транспорте (по видам). | ОПК-9.2.1.1 | знает особенности эксплуатации систем защиты информации автоматизированных систем на транспорте | Информационная безопасность автоматизированных систем на транспорте | ПС 06.033- ОТФ С,  ТФ В/02.6 |
| ОПК-9.2.2.1 | умеет осуществлять внедрение систем защиты информации автоматизированных систем на транспорте |
| ОПК-9.2.3.1 | Владеет методами эксплуатации систем защиты информации автоматизированных систем на транспорте |
| ОПК-9.2.1.2 | знает особенности эксплуатации систем защиты информации информационно-управляющих и информационно-логистических систем на транспорте | Информационная безопасность информационно-управляющих и информационно-логистических систем на транспорте |
| ОПК-9.2.2.2 | умеет осуществлять внедрение систем защиты информации информационно-управляющих и информационно-логистических систем на транспорте, в том числе автоматизированных систем управления технологическими процессами |
| ОПК-9.2.3.2 | Владеет методами эксплуатации систем защиты информации информационно-управляющих и информационно-логистических систем на транспорте, в том числе автоматизированных систем управления технологическими процессами |
| ОПК-9.2.1.3 | знает особенности эксплуатации систем защиты информации корпоративных сетей передачи данных (по видам транспорта) | Технология защиты в корпоративных сетях передачи данных (по видам транспорта) |
| ОПК-9.2.2.3 | умеет осуществлять внедрение систем защиты информации корпоративных сетей передачи данных (по видам транспорта) |
| ОПК-9.2.3.3 | Владеет методами эксплуатации систем защиты информации корпоративных сетей передачи данных (по видам транспорта) |
| ОПК-9.3. Способен осуществлять контроль защищенности автоматизированных, информационно-управляющих и информационно-логистических систем на транспорте (по видам) с учетом установленных требований безопасности. | ОПК-9.3.1.1 | знает основные угрозы и уязвимости, методы контроля защищенности автоматизированных систем на транспорте | Информационная безопасность автоматизированных систем на транспорте | ПС 06.033- ОТФ В, ТФ С/03.6, D/01.7 |
| ОПК-9.3.2.2 | умеет анализировать, прогнозировать и устранять угрозы информационной безопасности автоматизированных систем на транспорте в течение всего времени их применения |
| ОПК-9.3.3.1 | владеет навыками применения автоматизированных средств контроля защищенности автоматизированных систем на транспорте |
| ОПК-9.3.1.2 | знает основные угрозы и уязвимости, методы контроля защищенности информационно-управляющих и информационно-логистических систем на транспорте | Информационная безопасность информационно-управляющих и информационно-логистических систем на транспорте |
| ОПК-9.3.2.3 | умеет анализировать, прогнозировать и устранять угрозы информационной безопасности информационно-управляющих и информационно-логистических систем на транспорте, в том числе автоматизированных систем управления технологическими процессами, в течение всего времени их применения |
| ОПК-9.3.3.2 | владеет навыками применения автоматизированных средств контроля защищенности информационно-управляющих и информационно-логистических систем на транспорте, в том числе автоматизированных систем управления технологическими процессами |
| ОПК-9.3.1.3 | знает основные дефекты и уязвимости программного обеспечения автоматизированных систем на транспорте | Анализ безопасности программного обеспечения автоматизированных систем на транспорте |
| ОПК-9.3.2.1 | умеет выявлять дефекты и уязвимости в программном обеспечении автоматизированных систем на транспорте |
| ОПК-9.3.3.3 | владеет навыками применения инструментальных средств анализа безопасности программного обеспечения автоматизированных систем на транспорте |
| ОПК-9.3.1.4 | знает основные угрозы и уязвимости, методы контроля защищенности корпоративных сетей передачи данных (по видам транспорта) | Технология защиты в корпоративных сетях передачи данных (по видам транспорта) |
| ОПК-9.3.2.4 | умеет анализировать, прогнозировать и устранять угрозы информационной безопасности корпоративных сетей передачи данных (по видам транспорта) |
| ОПК-9.3.3.4 | владеет навыками применения инструментальных средств контроля защищенности корпоративных сетей передачи данных (по видам транспорта) |
| ОПК-10.1. Способен планировать, разрабатывать и осуществлять мероприятия по обеспечению безопасности автоматизированных систем управления технологическими процессами. | ОПК-10.1.1.1. | знает модель угроз информационной безопасности на предприятии (объекте) топливно-энергетического комплекса | Планирование мероприятий по защите АСУ ТП | ПС  ОТФ А, ТФ А/01.6 ПС  ОТФ D, ТФ D/02.7 |
| ОПК-10.1.1.2 | знает локальные нормативные акты и другие документы, определяющие политику и правила обеспечения информационной безопасности на предприятии (объекте) топливно-энергетического комплекса |
| ОПК-10.1.2.1 | умеет классифицировать и оценивать угрозы безопасности информации для значимых объектов критической информационной инфраструктуры на предприятии (объекте) топливно-энергетического комплекса |
| ОПК-10.1.2.2 | умеет разрабатывать модели угроз безопасности информации и нарушителей в значимых объектах критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| ОПК-10.1.2.3 | умеет определять информационную инфраструктуру и информационные ресурсы значимых объектов критической информационной инфраструктуры объектов топливно-энергетического комплекса, подлежащие защите |
| ОПК-10.2. Способен проектировать системы защиты информации автоматизированных систем управления технологическими процессами с учетом установленных требований безопасности | ОПК-10.2.1.1. | знает этапы проектирования систем защиты информации критически важных объектов; | Проектирование, разработка и реализация систем защиты информации АСУ ТП | ПС  ОТФ А, ТФ А/02.6 ПС  ОТФ А, ТФ А/03.6 |
| ОПК-10.2.1.2 | знает основные методические и руководящие документы по защите информации на значимых объектах критической информационной инфраструктуры |
| ОПК-10.2.1.3 | знает основную эксплуатационную и проектную документацию на информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, обеспечивающие функционирование топливно-энергетического комплекса |
| ОПК-10.2.2.1 | умеет выбирать меры защиты информации, подлежащие реализации в системе защиты информации значимых объектов критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| ОПК-10.2.2.2 | умеет выбирать программно-аппаратные средства защиты информации для использования их в составе значимых объектов критической информационной инфраструктуры топливно-энергетического комплекса с целью обеспечения требуемого уровня защищенности информации; |
| ОПК-10.2.3.1 | владеет навыками определения комплекса мер для защиты информации значимых объектов критической информационной инфраструктуры топливно-энергетического комплекса |
| ОПК-10.3. Способен организовывать и осуществлять контроль защищенности автоматизированных систем управления технологическими процессами. | ОПК-10.3.1.1 | знает технические средства контроля эффективности мер защиты информации | Организация информационной безопасности АСУ ТП | ПС  ОТФ В, ТФ В/02.6 ПС  ОТФ С, ТФ С/01.6 ПС  ОТФ С, ТФ С/03.6 |
| ОПК-10.3.1.2 | знает модель нарушителя информационной безопасности на предприятии (объекте) топливно-энергетического комплекса |
| ОПК-10.3.1.3 | знает основные системы и способы тестирования на проникновение |
| ОПК-10.3.2.1 | умеет определять источники и причины возникновения инцидентов |
| ОПК-10.3.2.2 | умеет обнаруживать нарушения правил разграничения доступа |
| ОПК-10.3.2.3 | умеет определять защищенность значимых объектов критической информационной инфраструктуры в соответствии с требованиями по безопасности |
| ОПК-11.1. Способен планировать и разрабатывать меры по обеспечению безопасности значимых объектов критической информационной инфраструктуры | ОПК-11.1.1.1 | знает методику моделирования угроз информационной безопасности | Планирование мероприятий по защите ЗО КИИ | ПС  ОТФ А, ТФ А/01.6 ПС  ОТФ D, ТФ D/02.7 |
| ОПК-11.1.1.2 | знает локальные нормативные акты и другие документы, определяющие политику и правила обеспечения информационной безопасности на предприятии (объекте) топливно-энергетического комплекса |
| ОПК-11.1.2.1 | умеет классифицировать и оценивать угрозы безопасности информации для значимых объектов критической информационной инфраструктуры на предприятии (объекте) топливно-энергетического комплекса |
| ОПК-11.1.2.2 | умеет разрабатывать модели угроз безопасности информации и нарушителей в значимых объектах критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| ОПК-11.1.1.3 | умеет определять информационную инфраструктуру и информационные ресурсы значимых объектов критической информационной инфраструктуры объектов топливно-энергетического комплекса, подлежащие защите |
| ОПК-11.2. Способен обеспечить функционирование систем безопасности значимых объектов критической информационной инфраструктуры | ОПК-11.2.1.1 | знает этапы проектирования систем защиты информации ЗО КИИ | Проектирование, разработка и реализация систем защиты ЗО КИИ | ПС  ОТФ А, ТФ А/02.6 ПС  ОТФ А, ТФ А/03.6 |
| ОПК-11.2.1.2 | знает основные методические и руководящие документы по защите информации на ЗО КИИ |
| ОПК-11.2.1.3 | знает основную эксплуатационную и проектную документацию информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, обеспечивающие функционирование топливно-энергетического комплекса |
| ОПК-11.2.2.1 | умеет выбирать меры защиты информации, подлежащие реализации в системе защиты информации ЗО КИИ объектов ТЭК |
| ОПК-11.2.2.2 | умеет выбирать программно-аппаратные средства защиты информации для использования их в составе значимых объектов критической информационной инфраструктуры топливно-энергетического комплекса с целью обеспечения требуемого уровня защищенности информации; |
| ОПК-11.2.3.1 | владеет навыками определения комплекса мер для защиты информации значимых объектов критической информационной инфраструктуры топливно-энергетического комплекса |
| ОПК-11.3. Способен организовывать и осуществлять меры по контролю состояния безопасности значимых объектов критической информационной инфраструктуры | ОПК-11.3.1.1 | знает технические средства контроля эффективности мер защиты информации | Аудит и оценка защищенности информационной безопасности | ПС  ОТФ В, ТФ В/02.6 ПС  ОТФ С, ТФ С/01.6 ПС  ОТФ С, ТФ С/03.6 |
| ОПК-11.3.1.2 | знает модель нарушителя информационной безопасности на предприятии (объекте) топливно-энергетического комплекса |
| ОПК-11.3.1.3 | знает основные системы и способы тестирования на проникновение |
| ОПК-11.3.2.1 | умеет определять источники и причины возникновения инцидентов |
| ОПК-11.3.2.2 | умеет обнаруживать нарушения правил разграничения доступа |
| ОПК-11.3.2.3 | умеет определять защищенность значимых объектов критической информационной инфраструктуры в соответствии с требованиями по безопасности |

**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.

Объем обязательной части составляет не менее - 280 з.е.

**5.2. Рекомендуемые типы практики**

В Блок 2 «Практика» входят учебная и производственная практики (далее вместе - практики).

Типы учебной практики:

* учебно-лабораторный практикум;
* ознакомительная практика;
* экспериментально-исследовательская практика.

Типы производственной практики:

* технологическая практика;
* проектно-технологическая практика;
* эксплуатационная практика;
* научно-исследовательская работа;
* преддипломная практика.

Способы проведения практик:

* стационарная;
* выездная.

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

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

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Индекс | Наименование дисциплин (модулей), практик, аттестационных испытаний | Форма промежуточной аттестации | Трудоемкость | | | Коды формируемых компетенций |
| з.е.\* | часы | |
| Всего | Контактная работа |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |

| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| --- | --- | --- | --- | --- | --- | --- |
| Б.1 | Блок 1. Дисциплины (модули) |  | Не  менее  282 | Не  менее  10480 | Не  менее  5240 |  |
| Б.1.О | Обязательная часть |  | Не  менее 236 |  |  |  |
| Б.1.О.1 | История (История России, Всеобщая история) | экзамен | 5 | 180 | 72 | УК-5, ОПК-16 |
| Б.1.О.2 | Физическая культура | 2 зачета | 2 | 72 | 36 | УК-7 |
| Б.1.О.3 | Иностранный язык | 2 зачета,  экзамен | 11 | 396 | 216 | УК-4 |
| Б.1.О.4 | Экономика | экзамен | 4 | 144 | 72 | УК-9,  УК-10 |
| Б.1.О.5 | Философия | зачет, экзамен | 5 | 180 | 108 | УК-1, УК-5 |
| Б.1.О.6 | Безопасность жизнедеятельности | зачет | 2 | 72 | 54 | УК-8 |
| Б.1.О.7 | Основы управления проектами | зачет | 3 | 108 |  | УК-1, УК-2, УК-3, УК-6 |
| Группа учебных дисциплин (модулей) "Математические науки" | | | | | | |
| Б.1.О.8 | Математический анализ | 3 экзамена | 13 | 468 |  | ОПК-3 |
| Б.1.О.9 | Теория вероятностей и математическая статистика | зачет, экзамен | 7 | 252 |  | ОПК-3 |
| Б.1.О.10 | Алгебра и геометрия | 2 экзамена | 9 | 324 |  | ОПК-3 |
| Б.1.О.11 | Дискретная математика | зачет, экзамен | 8 | 288 |  | ОПК-3 |
| Б.1.О.12 | Теория информации (Теория информации и кодирования) | зачет | 3 | 108 |  | ОПК-3, ОПК-4 |
| Группа учебных дисциплин (модулей)  "Физико-технические основы информационных технологий" | | | | | | |
| Б.1.О.13 | Физика | 3 экзамена | 13 | 468 |  | ОПК-4 |
| Б.1.О.14 | Электроника и схемотехника | экзамен | 6 | 216 |  | ОПК-4 |
| Б.1.О.15 | Организация ЭВМ и вычислительных систем (Аппаратные средства вычислительной техники) | 2 экзамена,  курсовая работа | 9 | 324 |  | ОПК-4, ОПК-13 |
| Б.1.О.16 | Сети и системы передачи информации | экзамен | 5 | 180 |  | ОПК-9 |
| Группа учебных дисциплин (модулей)  "Информационные технологии и программирование" | | | | | | |
| Б.1.О.17 | Языки программирования | зачет, экзамен | 9 | 324 |  | ОПК-7 |
| Б.1.О.18 | Технологии и методы программирования | зачет, экзамен | 9 | 324 |  | ОПК-7 |
| Б.1.О.19 | Безопасность операционных систем | зачет, экзамен | 10 | 360 |  | ОПК-10, ОПК-12, ОПК-15 |
| Б.1.О.20 | Безопасность вычислительных сетей | зачет, экзамен | 10 | 360 |  | ОПК-10, ОПК-12, ОПК-15 |
| Б.1.О.21 | Безопасность систем баз данных | зачет, экзамен | 10 | 360 |  | ОПК-12, ОПК-15 |
| Группа учебных дисциплин (модулей)  "Методы и средства обеспечения информационной безопасности автоматизированных систем" | | | | | | |
| Б.1.О.22 | Основы информационной безопасности | зачет | 3 | 108 |  | ОПК-1 |
| Б.1.О.23 | Организационное и правовое обеспечение информационной безопасности | экзамен | 5 | 180 |  | ОПК-5, ОПК-6, ОПК-14 |
| Б.1.О.24 | Защита информации от утечки по техническим каналам | экзамен | 5 | 180 |  | ОПК-5, ОПК-6, ОПК-13 |
| Б.1.О.25 | Методы и средства криптографической защиты информации | экзамен | 5 | 180 |  | ОПК-10 |
| Б.1.О.26 | Программно-аппаратные средства защиты информации | экзамен | 6 | 216 |  | ОПК-9 |
| Б.1.О.27 | Управление информационной безопасностью | экзамен | 5 | 180 |  | ОПК-5, ОПК-15 |
| Б.1.О.28 | Разработка и эксплуатация автоматизированных систем в защищенном исполнении | экзамен | 6 | 216 |  | ОПК-11, ОПК-13, ОПК-14 |
|  | Элективные дисциплины по физической культуре и спорту |  |  | 328 |  | УК-7 |
|  | Дисциплины (модули) образовательной организации  (при необходимости) |  |  |  |  |  |
|  | Элективные дисциплины (модули) образовательной организации (при необходимости) |  |  |  |  |  |
| Б.1.С | Дисциплины (модули) специализации (перечень, трудоемкость и распределение дисциплин (модулей) по периодам обучения определяется образовательной организацией) |  | Не  менее 21 | Не  менее 756 | Не  менее  350 |  |
|  | специализация № 1 "Автоматизированные информационные системы 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. |  |  |  |  |  |
|  | специализация № 2 "Высокопроизводительные вычислительные системы 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. |  |  |  |  |  |
|  | специализация № 3 "Специальные технологии обеспечения информационной безопасности" |  |  |  |  |  |
|  | 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 "Безопасность автоматизированных систем критически важных объектов" |  |  |  |  | ОПК-4.1-ОПК-4.3 |
| Б.1.С.4.1 | Информационная безопасность автоматизированных систем критически важных объектов | экзамен | 6 | 216 | 108 | ОПК 4.1 |
| Б.1.С.4.2 | Мониторинг информационной безопасности критически важных объектов | экзамен | 5 | 180 | 96 | ОПК-4.2, ОПК-4.3 |
| Б.1.С.4.3 | Основы построения средств и комплексов обеспечения информационной безопасности | зачет с оценкой | 4 | 144 | 72 | ОПК 4.3 |
| Б.1.С.4.4 | Дисциплины (модули) образовательной организации  (при необходимости) |  |  |  |  |  |
| Б.1.С.5 | специализация № 5 "Безопасность открытых информационных систем" |  |  |  |  | ОПК-5.1-ОПК-5.2 |
| Б.1.С.5.1 | Криптографические протоколы и стандарты | экзамен | 6 | 216 | 108 | ОПК-5.1 |
| Б.1.С.5.2 | Информационная безопасность открытых систем | экзамен | 5 | 180 | 96 | ОПК-5.2 |
| Б.1.С.5.3 | Открытые информационные системы | экзамен | 6 | 216 | 108 | ОПК-5.3 |
| Б.1.С.5.4 | Дисциплины (модули) образовательной организации  (при необходимости) |  |  |  |  |  |
| Б.1.С.6 | специализация № 6 "Безопасность автоматизированных систем в кредитно-финансовой сфере" |  |  |  |  | ОПК 6.1-6.3 |
| Б.1.С.6.1 | Платежные системы и их безопасность | зачет | 4 | 144 | 72 | ОПК-6.1 |
| Б.1.С.6.2 | Нормативная база обеспечения информационной безопасности организаций финансово-кредитной сферы | экзамен, зачет с оценкой | 6 | 216 | 108 | ОПК-6.3 |
| Б.1.С.6.3 | Управление инцидентами и непрерывностью бизнеса в организациях финансово-кредитной сферы | зачет | 4 | 144 | 72 | ОПК-6.2 |
| Б.1.С.6.4 | Защита информации в автоматизированных системах организаций финансово-кредитной сферы | экзамен | 5 | 180 | 96 | ОПК-6.3 |
| Б.1.С.6.5 | Дисциплины (модули) образовательной организации  (при необходимости) |  |  |  |  |  |
| Б.1.С.7 | специализация № 7 "Анализ безопасности информационных систем" |  |  |  |  | ОПК 7.1-7.3 |
| Б.1.С.7.1 | Верификация безопасности информационных систем | экзамен | 5 | 180 | 96 | ОПК-7.2 |
| Б.1.С.7.2 | Анализ рисков информационной безопасности | экзамен | 6 | 216 | 108 | ОПК-7.3 |
| Б.1.С.7.3 | Анализ безопасности информационных систем | экзамен | 6 | 216 | 108 | ОПК-7.1 |
| Б.1.С.7.4 | Дисциплины (модули) образовательной организации  (при необходимости) |  |  |  |  |  |
| Б.1.С.8 | специализация № 8 "Разработка автоматизированных систем в защищенном исполнении" |  |  |  |  | ОПК-8.1-ОПК-8.3 |
| Б.1.С.8.1 | Администрирование автоматизированных систем в защищенном исполнении | экзамен | 6 | 216 | 108 | ОПК-8.1 |
| Б.1.С.8.2 | Организация проектной деятельности | экзамен | 5 | 180 | 96 | ОПК-8.2 |
| Б.1.С.8.3 | Информационная безопасность автоматизированных систем в защищенном исполнении | экзамен | 6 | 216 | 108 | ОПК-8.3 |
| Б.1.С.8.4 | Дисциплины (модули) образовательной организации  (при необходимости) |  |  |  |  |  |
| Б.1.С.9 | специализация № 9 "Безопасность автоматизированных систем на транспорте" (по видам) |  |  |  |  | ОПК 9.1-9.3 |
| Б.1.С.9.1 | Информационная безопасность автоматизированных систем на транспорте | экзамен | 6 | 216 | 96 | ОПК-9.1, ОПК-9.2, ОПК-9.3 |
| Б.1.С.9.2 | Информационная безопасность информационно-управляющих и информационно-логистических систем на транспорте | экзамен | 5 | 180 | 80 | ОПК-9.1, ОПК-9.2, ОПК-9.3 |
| Б.1.С.9.3 | Анализ безопасности программного обеспечения автоматизированных систем на транспорте | экзамен | 6 | 216 | 96 | ОПК-9.1, ОПК-9.3 |
| Б.1.С.9.4 | Технология защиты в корпоративных сетях передачи данных (по видам транспорта) | экзамен | 4 | 144 | 80 | ОПК-9.1, ОПК-9.2, ОПК-9.3 |
| Б.1.С.10 | специализация № 10 "Безопасность автоматизированных систем управления технологическими процессами" (по отрасли или в сфере профессиональной деятельности) |  |  |  |  | ОПК-10.1-10.3 |
| Б.1.С.10.1 | Планирование мероприятий по защите АСУ ТП | экзамен | 6 | 216 | 108 | ОПК-10.1 |
| Б.1.С.10.2 | Проектирование, разработка и реализация систем защиты информации АСУ ТП | экзамен | 6 | 216 | 108 | ОПК-10.2 |
| Б.1.С.10.3 | Организация информационной безопасности АСУ ТП | экзамен | 5 | 180 | 96 | ОПК-10.3 |
| Б.1.С.10.4 | Дисциплины (модули) образовательной организации  (при необходимости) |  |  |  |  |  |
| Б.1.С.11 | специализация № 11 "Безопасность значимых объектов критической информационной инфраструктуры" (по отрасли или в сфере профессиональной деятельности) |  |  |  |  | ОПК 11.1-11.3 |
| Б.1.С.11.1 | Планирование мероприятий по защите ЗО КИИ | экзамен | 6 | 216 | 108 | ОПК- 11.1 |
| Б.1.С.11.2 | Проектирование, разработка и реализация систем защиты ЗО КИИ | экзамен | 6 | 216 | 108 | ОПК-11.2 |
| Б.1.С.11.3 | Аудит и оценка защищенности информационной безопасности | экзамен | 5 | 180 | 96 | ОПК- 11.3 |
| Б.1.С.11.4 | 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 | | | | | | |
| Б.1.В.1 | Основы научных исследований | зачет | 2 | 72 | 42 | ОПК-8 |
| Б.1.В.2 | Информатика | зачет | 3 | 108 | 64 | ОПК-2 |
| Б.1.В.3 | Инженерная и компьютерная графика (Инженерная графика) | зачет | 2 | 72 | 42 | ОПК-5 |
| Элективные дисциплины (модули) образовательной организации (при необходимости) | | | | | | |
| Б.2 | Блок 2. Практика |  | Не  менее  27 |  |  |  |
| Б.2.О | Обязательная часть |  | Не  менее  12 |  |  |  |
| Б.2.О.1 | Производственная (преддипломная) практика |  | Не  менее  12 |  |  | УК-2, УК-4, УК-6,  ОПК-8, ОПК-11 |
|  | Учебная и производственная практики, определяемые образовательной организацией (при необходимости) |  |  |  |  |  |
| Б.2.В | Часть, формируемая участниками образовательных отношений |  |  |  |  |  |
|  | Учебная и производственная практики, определяемые образовательной организацией (при необходимости) |  |  |  |  |  |
| Б.3 | Блок 3. Государственная итоговая аттестация |  | Не  менее  6 | Не  менее  216 |  |  |
| Б.3.О | Обязательная часть |  | Не  менее  6 | Не  менее  216 |  |  |
| Б.3.О.1 | Подготовка к защите и защита выпускной квалификационной работы |  | 6 | 216 |  |  |
|  | Итого по образовательной программе |  | 330 | 12208 |  |  |

Образовательная организация в пределах требований, установленных ФГОС, при формировании образовательной программы высшего образования в отношении учебных дисциплин (модулей), указанных в настоящем примерном учебном плане, вправе: конкретизировать наименование; увеличивать трудоемкость; уменьшать трудоемкость не более чем на 2 з.е. при условии, что итоговая величина составит не менее 3 з.е.; устанавливать периоды обучения, в которых изучается учебная дисциплина (модуль), а также формы промежуточной аттестации по их окончании; разделять учебные дисциплины (модули) при условии сохранения общей трудоемкости и индикаторов достижениия формируемых компетенций, установленных примерной основной образовательной программой для исходной учебной дисциплины (модуля).

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.

**5.4. 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 приведены в таблице 5.

Таблица 5

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 |

Управление воспитательной работой.

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 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.

**5.5. Примерный календарный план воспитательной работы**

Календарный план воспитательной работы Организации включает перечень основных мероприятий по направлениям воспитательной работы.

Примерная форма плана представлена в таблице 6.

Таблица 6

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 |

| 1 | 2 | 3 | 4 | 5 |
| --- | --- | --- | --- | --- |
| 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 |  |  |  |

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

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

Коды формируемых компетенций: *УК-5, ОПК-16*

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: не менее 180 ч.

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.

Рекомендуемый перечень основной литературы:

1. Орлов А.С., Георгиев В.А., Н.Г. Георгиева, Сивохина Т.А. История России. – М.: Проспект, 2016;

2. Зуев М.Н., Чернобаев А.А. История России. – М.: Высшая школа, 2009;

3. Дворниченко А.Ю., Тот Ю.В., Ходяков М.В. История России. – М.: Проспект, 2010.

Перечень материально-технического обеспечения:

Специфического материально-технического обеспечения не требуется.

*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: не менее 72 ч.

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.

Рекомендуемый перечень основной литературы:

1. Муллер А.Б. Физическая культура. – М.: Издательство Юрайт, 2014;

2. Кошелев В.Ф., Малоземов О.Ю., Бердникова Ю.Г., Минаев А.В., Филимонова С.И. Физическое воспитание студентов в техническом вузе. – Екатеринбург: Изд-во АМБ, 2015.

Перечень материально-технического обеспечения:

Специфического материально-технического обеспечения не требуется.

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

Коды формируемых компетенций: *УК-4*

В результате изучения дисциплины студент должен

знать:

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

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: не менее 396 ч.

Форма контроля: *2 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.

Рекомендуемый перечень основной литературы:

1. Буров Р.И., Бузин А.Ю., Илларионов Б.В. Теория информации. Учебник. – Воронеж: ВУНЦ ВВС «ВВА», 2019. – 164 с.

2. Электронное учебное издание по дисциплине «Теория информации». Тео-рия информации. № 4186 от 18.06.2021 г.

Перечень материально-технического обеспечения:

Специфического материально-технического обеспечения не требуется.

*Б.1.О.4 Дисциплина «Экономика»*

Коды формируемых компетенций: *УК-9, 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: не менее 144 ч.

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.

Рекомендуемый перечень основной литературы:

1. Лобачева Е.Н. Экономическая теория. – М.: Издательство Юрайт, 2019;

2. Салов А.И. Экономика. – М.: Литера, 2017;

3. Гребенников П.И. Экономика. – СПб.: Питер, 2019.

Перечень материально-технического обеспечения:

Специфического материально-технического обеспечения не требуется.

*Б.1.О.5 Дисциплина «Философия»*

Коды формируемых компетенций: *УК-1, УК-5*

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: не менее 180 ч.

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.

Рекомендуемый перечень основной литературы:

1. Зотов А.Ф., Разин А.В., Миронов В.В. Философия. – М.: Проспект, 2020;

2. Чумаков А.Н. Философия. – М.: Проспект, 2021;

3. Алексеев П.В., Панин А.В. Философия. – М.: Проспект, 2021.

Перечень материально-технического обеспечения:

Специфического материально-технического обеспечения не требуется.

*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: не менее 72 ч.

Форма контроля: *зачет*

Содержание дисциплины:

Комфортные и допустимые условия жизнедеятельности. Введение в БЖД: цель, задачи и содержание дисциплины, ее место и роль среди других наук и в подготовке специалиста; проблема обеспечения безопасности человека в системе «человек - среда обитания»; концепция рисков. Микроклимат и воздушная среда рабочей зоны: влияние микроклимата на работоспособность человека; нормирование параметров микроклимата в конкретном производстве; тепловые излучения и влияние их на организм человека; нормирование тепловых излучений; адаптация и акклиматизация в условиях перегревания и переохлаждения; отопление, вентиляция и кондиционирование воздуха; естественная и механическая вентиляция. Действие вредных веществ на организм человека в конкретном производстве. Нормирование концентрации вредных веществ в воздушной среде рабочей зоны. Методы контроля состояния воздушной среды. Производственный шум: источники шума и шумовые характеристики в конкретном производстве; производственная вибрация; физические характеристики и измерение вибраций в конкретном производстве; характеристика и опасность совместного воздействия вибраций, шума, ультразвука и инфразвука. Производственное освещение: характеристика электрических источников света и осветительных приборов; естественное и совмещенное освещение в производственных цехах. Оптимизация параметров рабочих мест: виды и формы деятельности; энергетические затраты при различных формах деятельности; определение категории тяжести труда; способы оценки тяжести и напряженности трудовой деятельности; работоспособность и ее динамика; пути повышения эффективности трудовой деятельности; эргономические основы безопасности жизнедеятельности. Техногенные и природные чрезвычайные ситуации: прогнозирование параметров и оценка обстановки при ЧС; защитные мероприятия при ЧС; ликвидация последствий ЧС; защита от терроризма. Электробезопасность при эксплуатации электрических устройств и оборудования. Электробезопасность: действие электрического тока на организм человека; опасность поражения в различных электрических сетях; заземление и зануление; классификация помещений по электробезопасности; квалификационные группы персонала по электробезопасности; напряжение шага, прикосновения; защитные меры в электроустановках; защитные средства, применяемые в электроустановках; защитная изоляция: виды, роль в обеспечении электробезопасности, критические параметры; защита от статического электричества; организационные и технические мероприятия при эксплуатации электроустановок; средства индивидуальной защиты. Защита от электромагнитных полей высокой и сверхвысокой частоты: основные понятия и определения; физические характеристики электромагнитных полей (ЭМП); воздействие электромагнитных полей на организм человека; тепловой и функциональный эффект; органы человека с повышенной чувствительностью к ЭМП; организационные, технические и санитарно-гигиенические меры защиты от электромагнитных излучений в конкретном производстве; нормирование интенсивности ЭМП; расчет интенсивности ЭМП на рабочих местах в зависимости от параметров источника излучения и среды; определение границ опасной зоны. Защита от лазерных излучений: применение лазеров в технологических процессах; биологическое действие лазерного излучения: воздействие на глаза, кожу, внутренние органы и организм человека в целом; опасные и вредные производственные факторы, сопутствующие эксплуатации лазеров; основные способы и средства защиты от лазерного излучения: экранирование, блокировка, сигнализация, удаление рабочих мест из лазерно-опасной зоны; средства индивидуальной защиты. Радиационная безопасность: основные понятия, определения, единицы измерения в области радиационной безопасности; фоновое облучение человека; нормирование ионизирующих излучений; защита от воздействия ионизирующего излучения на производстве; средства индивидуальной защиты. Пожарная безопасность при эксплуатации электрических устройств: причины возникновения пожаров и взрывов в помещениях и в производственных процессах; опасные факторы при пожарах и взрывах; основные сведения из теории естественного окисления, теплового самовоспламенения и цепных реакций; самовоспламенение смеси газов, воспламенение жидкости, вспышка паров; оценка пожароопасности веществ и материалов; предупреждение взрывов и пожаров; ликвидация их последствий; показатели пожароопасности; классификация зданий и помещений по пожарной (взрывной) опасности; прогнозирование пожаров и взрывов; пожарная безопасность в технологических процессах конкретных производств; системы и средства пожаротушения, пожарной автоматики и сигнализации; средства индивидуальной защиты; правила эвакуации лиц, пострадавших на пожарах, в газоотравленных зонах, при отравлениях. 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: ранение, ожоги, обморожения, переломы, вывихи, растяжения связок; условия успеха при оказании первой помощи: быстрота оказания помощи, обученность персонала методам оказания первой медицинской помощи.

Рекомендуемый перечень лабораторных работ:

* измерение освещенности
* измерение уровня шума
* 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. – СПб.: Питер, 2013;

3. Каракиян В.И., Никулина И.М. Безопасность жизнедеятельности. – М.: Юрайт, 2015. "

Перечень материально-технического обеспечения:

Для проведения лабораторных работ требуется учебная лаборатория, оборудованная стендами и установками Российского научно-производственного объединения «Росучприбор» или аналогичными:

– «Звукоизоляция и звукопоглощение БЖ2МП»;

– «Эффективность и качество освещения БЖ1МП»;

– «Электробезопасность трехфазных сетей переменного тока БЖ6/1»;

– «Защита от СВЧ излучения БЖ5МП»;

– «Максим 3». Тренажер оказания первой медицинской помощи с пультом управления и настенным табло.

*Б.1.О.7 Дисциплина «Основы управления проектами»*

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

В результате изучения дисциплины студент должен

знать:

* основные источники информации о проблемных ситуация 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: не менее 108 ч.

Форма контроля: *зачет*

Перечень материально-технического обеспечения:

Специфического материально-технического обеспечения не требуется.

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

Коды формируемых компетенций: *ОПК-3*

В результате изучения дисциплины студент должен

знать:

* основные понятия теории пределов и непрерывности функций одной и нескольких действительных переменных;
* основные методы дифференциального исчисления функций одной и нескольких действительных переменных;
* основные методы интегрального исчисления функций одной и нескольких действительных переменных;
* основные методы исследования числовых и функциональных рядов;
* основные задачи теории функций комплексного переменного;
* основные типы обыкновенных дифференциальных уравнений и методы их решения

уметь:

* исследовать функциональные зависимости, возникающие для решения стандартных прикладных задач;
* использовать типовые модели и методы математического анализа для решения стандартных прикладных задач;
* проводить типовые расчеты с использованием основных формул дифференциального и интегрального исчисления;
* пользоваться справочными материалами по математическому анализу.

Примерное распределение часов: не менее 468 ч.

Форма контроля: *3 экзамена*

Содержание дисциплины:

Понятие множества и функции. Действительные числа. Действительные числа. Понятие функции. Предел функции одной переменной. Непрерывность функции одной переменной. Дифференциальное исчисление функции одной переменной. Неопределенный интеграл. Определенный интеграл. Несобственный интеграл. Дифференциальное исчисление функций многих действительных переменных. Числовые ряды. Функциональные последовательности и ряды. Ряды Фурье. Кратные и криволинейные интегралы. Обыкновенные дифференциальные уравнения. Дифференциальные уравнения в частных производных. Уравнения математической физики. Основные функции комплексного переменного.Дифференцирование и интегрирование функций комплексного переменного. Ряды в комплексной плоскости. Классификация особых точек. Вычисление интегралов при помощи вычетов. Операционное исчисление.

Перечень материально-технического обеспечения:

Специфического материально-технического обеспечения не требуется.

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

Коды формируемых компетенций: *ОПК-3*

В результате изучения дисциплины студент должен

знать:

* основные понятия теории вероятностей, числовые и функциональные характеристики распределений случайных величин и их основные свойства;
* классические предельные теоремы теории вероятностей;
* основные понятия теории случайных процессов;
* постановку задач и основные понятия математической статистики;
* стандартные ме­тоды получения точечных и интервальных оценок параметров вероятностных распределений;
* стандартные методы проверки статистических гипотез

уметь:

* применять стандартные вероятностные и статистические мо­дели для решения типовых прикладных задач;
* пользоваться стандартными вероятностно-статистическими методами анализа экспериментальных данных;
* строить стандартные процедуры принятия решений на основе имеющихся экспериментальных данных;
* использовать расчетные формулы и таблицы для решения стандартных вероятностно-статистических задач

Примерное распределение часов: не менее 252 ч.

Форма контроля: *зачет, экзамен*

Содержание дисциплины:

Элементы теории множеств, комбинаторики и теории меры. Аксиоматика теории вероятностей. Независимость событий и условные вероятности. Классические вероятностные схемы и классические предельные теоремы. Случайные величины и случайные векторы. Числовые характеристики случайных величин. Характеристические функции. Многомерное нормальное распределение. Сходимость случайных величин и предельные теоремы. Вероятностный метод в приложении к задачам комбинаторики и теории двоичных функций. Основные понятия математической статистики. Точечное оценивание параметров распределений. Интервальное оценивание параметров распределений. Проверка статистических гипотез по выборкам фиксированного объема (параметрическая статистика). Проверка статистических гипотез по выборкам фиксированного объема (непараметрическая статистика). Последовательный статистический анализ. Метод статистических испытаний. Стационарные случайные процессы. Дискретные цепи Маркова. Марковские процессы с непрерывным временем. Пуассоновский и винеровский процессы.

Перечень материально-технического обеспечения:

Специфического материально-технического обеспечения не требуется.

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

Коды формируемых компетенций: *ОПК-3*

В результате изучения дисциплины студент должен

знать:

* основные понятия и задачи векторной алгебры и аналитической геометрии;
* основные свойства алгебраических структур;
* основы линейной алгебры над произвольными полями

уметь:

* строить и изучать математические модели конкретных явлений и процессов для решения расчетных и исследовательских задач;
* решать основные задачи векторной алгебры и аналитической геометрии;
* решать основные задачи линейной алгебры, системы линейных уравнений над полями;
* использовать методы аналитической геометрии и векторной алгебры в смежных дисциплинах и физике;
* использовать методы линейной алгебры для решения прикладных задач

Примерное распределение часов: не менее 324 ч.

Форма контроля: *2 экзамена*

Содержание дисциплины:

Теория определителей и систем линейных уравнений. Векторная алгебра. Системы координат. Прямая линия на плоскости. Линии второго порядка на плоскости. Прямая и плоскость в пространстве. Поверхности второго порядка. Основные алгебраические структуры. Матрицы над кольцами. Определители матриц. Матрицы над полями и системы линейных уравнений. Линейная зависимость векторов арифметических пространств. Подпространства арифметических пространств. Числовые кольца и поля. Кольца вычетов. Кольца многочленов. Линейные пространства.

Рекомендуемый перечень основной литературы:

1. Ильин, В. А. Аналитическая геометрия: учебник / В. А. Ильин, Э. Г. По-зняк. - 7-е изд., стер. – Москва: ФИЗМАТЛИТ, 2009. – 224 с.

2. Ильин, В. А. Линейная алгебра: учебник / В. А. Ильин, Э. Г. Позняк. - 6-е изд., стер. – Москва: ФИЗМАТЛИТ, 2007. – 280 с.

Перечень материально-технического обеспечения:

Специфического материально-технического обеспечения не требуется.

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

Коды формируемых компетенций: *ОПК-3*

В результате изучения дисциплины студент должен

знать:

* свойства основных дискретных структур: конечных полей, графов, конечных автоматов, комбинаторных структур;
* основные понятия и методы теории графов;
* основные понятия и методы теории конечных автоматов;
* основные понятия и методы комбинаторного анализа

уметь:

* решать задачи периодичности и эквивалентности для конечных автоматов;
* применять аппарат производящих функций и рекуррентных соотношений для решения перечислительных задач;
* решать оптимизационные задачи на графах;
* применять стандартные методы дискретной математики для решения профессиональных задач;
* решать типовые комбинаторные и теоретико-графовые задачи;
* использовать язык и средства дискретной математики для решения профессиональных задач

Примерное распределение часов: не менее 288 ч.

Форма контроля: *зачет, экзамен*

Содержание дисциплины:

Основы комбинаторики. Бинарные отношения. Метод включения-исключения. Рекуррентных соотношений и метод производящих функций. Конечные поля. Линейные и циклические коды. Основные понятия теории графов. Эйлеровы и гамильтоновы графы. Деревья. Метрические характеристики графа. Основные понятия теории автоматов. Эквивалентность автоматов. Эксперименты с автоматами. Линейные автоматы над конечным полем. Память автоматов.

Перечень материально-технического обеспечения:

Специфического материально-технического обеспечения не требуется.

*Б.1.О.12 Дисциплина «Теория информации (Теория информации и кодирования)»*

Коды формируемых компетенций: *ОПК-3, ОПК-4*

В результате изучения дисциплины студент должен

знать:

* основные понятия и определения теории информации;
* основные понятия, определения и принципы теории помехоустойчивого кодирования;
* основные способы кодирования информации

уметь:

* определять информационные характеристики системы передачи сообщений и каналов связи;
* решать типовые задачи кодирования и де-кодирования сообщений.

Примерное распределение часов: не менее 108 ч.

Форма контроля: *зачет*

Содержание дисциплины:

Количество информации. Энтропия, Источники информации. Источник сообщений как случайный процесс. Теоремы Шеннона об источниках сообщений. Оптимальное кодирование. Однозначно декодируемых и префиксные коды. Математические модели непрерывных каналов связи. Математические модели дискретно-непрерывных и дискретных каналов связи. Принципы помехоустойчивого кодирования, помехоустойчивые коды.

Рекомендуемый перечень основной литературы:

1. Буров Р.И., Бузин А.Ю., Илларионов Б.В. Теория информации. Учебник. – Воронеж: ВУНЦ ВВС «ВВА», 2019. – 164 с.

2. Электронное учебное издание по дисциплине «Теория информации». Тео-рия информации. № 4186 от 18.06.2021 г.

Перечень материально-технического обеспечения:

Специфического материально-технического обеспечения не требуется.

*Б.1.О.13 Дисциплина «Физика»*

Коды формируемых компетенций: *ОПК-4*

В результате изучения дисциплины студент должен

знать:

* основные законы механики;
* основные положения термодинамики и молекулярной физики;
* основные законы электричества и магнетизма;
* основные законы теории колебаний и волн, волновой оптики;
* основные принципы квантовой физики.

уметь:

* проводить физический эксперимент, обрабатывать его результаты и делать выводы о проделанной исследовательской работе;
* решать типовые прикладные физические задачи

Примерное распределение часов: не менее 468 ч.

Форма контроля: *3 экзамена*

Содержание дисциплины:

Механика материальной точки. Механика твердого тела. Статистическая термодинамика. Электричество. Магнетизм. Волны. Оптика. Квантовая оптика. Квантовая механика.

Рекомендуемый перечень лабораторных работ:

Изучение динамики поступательного движения твердых тел с помощью машины Атвуда.

Определение ускорения свободного падения тел с помощью оборотного маятника.

Изучение динамики плоского движения твердых тел с помощью маятника Максвелла.

Экспериментальное подтверждение закона Дюлонга и Пти.Исследование собственных колебаний в простом колебательном контуре.

Определение диэлектрической проницаемости твердых тел.

Изучение вихревого электрического поля.

Методы получения и исследования дифракционной картины.

Экспериментальное подтверждение закона Стефана – Больцмана.

Рекомендуемый перечень основной литературы:

1. Савельев И.В. Курс общей физики (в 3-х томах): учебное пособие для ву-зов / И. В. Савельев. – 4-е–11-е изд. – СПб: Лань, 2003–2011. Т.1 – 432 с. Т.2 – 496 с. Т.3 – 317 с.

Перечень материально-технического обеспечения:

Специфического материально-технического обеспечения не требуется.

*Б.1.О.14 Дисциплина «Электроника и схемотехника»*

Коды формируемых компетенций: *ОПК-4*

В результате изучения дисциплины студент должен

знать:

* основополагающие принципы работы элементов и функциональных узлов электронной аппаратуры.

уметь:

* анализировать компонентную базу электронной аппаратуры.

Примерное распределение часов: не менее 216 ч.

Форма контроля: *экзамен*

Содержание дисциплины:

Полупроводниковые приборы. Полупроводники. Электронно-дырочный переход. Переход металл-полупроводник. Диоды. Виды полупроводниковых диодов, особенности работы и параметры. Биполярные и полевые транзисторы: принципы работы, разновидности, параметры. Вольтамперные характеристики транзисторов и их эквивалентные схемы. Электронные ключи. Основные схемы ключей на биполярных и полевых транзисторах. Принципы функционирования и основные характеристики ключевых элементов. Цифровая схемотехника. Принципы дискретной обработки информации. Формы представления двоичных сигналов. Потенциальные, импульсные сигналы и их основные характеристики. Логические элементы. Статические и динамические модели логических элементов. Логические интегральные схемы. Разновидности логических интегральных схем. Параметры логических интегральных схем. Измерение параметров интегральных схем. Типовые схемотехнические решения, схемы включения. Триггеры. Триггерные устройства различных типов. Принципы построения интегральных триггеров. Функциональные узлы комбинационного и последовательностного типа. Функциональные узлы комбинационного типа (дешифраторы, мультиплексоры, шифраторы, демультиплексоры, сдвигатели, сумматоры, вычитатели, компараторы, схемы сравнения). Модели и принципы построения комбинационных схем. Функциональные узлы последовательностного типа (регистры, счетчики, накапливающие сумматоры). Комбинированные цифровые устройства: умножители, арифметико-логические устройства. Риски сбоя в последовательностных и комбинационных схемах. Типовые схемотехнические решения при проектировании функциональных узлов цифровых устройств. Схемотехника запоминающих устройств. Запоминающие устройства (ЗУ) различных типов и их характеристики. Динамические и статические ЗУ. Типовые схемотехнические решения полупроводниковых ЗУ.

Рекомендуемый перечень лабораторных работ:

* Исследование характеристик полупроводниковых диодов.
* Исследование характеристик биполярных транзисторов.
* Исследование работы цифровых логических элементов и узлов комбинационного типа.
* Исследование работы цифровых устройств последовательностного типа.

Рекомендуемый перечень основной литературы:

Гусев, В.Г. Электроника и микропроцессорная техника: учебник для вузов / В.Г. Гусев, Ю.М. Гусев. – Изд. 3-е, перераб. и доп. – М.: Высш. шк., 2004. – 790 с.

Перечень материально-технического обеспечения:

Специфического материально-технического обеспечения не требуется.

*Б.1.О.15 Дисциплина «Организация ЭВМ и вычислительных систем*

(Аппаратные средства вычислительной техники)»

Коды формируемых компетенций: ОПК-4, *ОПК-13*

В результате изучения дисциплины студент должен

знать:

* технические характеристики, основные показатели качества и эффективности ЭВМ и вычислительных систем, методы их оценки и пути совершенствования;
* терминологию, основные руководящие и регламентирующие документы в области ЭВМ и вычислительных систем

уметь:

* проводить анализ архитектуры и структуры ЭВМ и вычислительных систем;
* осуществлять сбор, обработку, анализ и систематизацию научно-технической информации в области ЭВМ и систем с применением современных информационных технологий

Примерное распределение часов: не менее 324 ч.

Содержание дисциплины:

Раздел 1. Архитектура ЭВМ последовательного типа

Тема 1. Базовые сведения в области ЭВМ и вычислительных систем

Основные понятия и определения в области ЭВМ и ВС. Классификация ЭВМ и ВС. Этапы и основные тенденции развития архитектуры ЭВМ и ВС. Характеристика основных классов ЭВМ: персональные, портативные, рабочие станции, серверы, супер-ЭВМ и другие. Показатели качества и эффективности функционирования ЭВМ и ВС. Методы и средства оценки производительности ЭВМ. Методы и средства повышения надежности ЭВМ.

Тема 2. Организация ЭВМ последовательного типа

Способы структурной организации ЭВМ. Типовая структура ЭВМ. Состав, назначение и принципы функционирования основных компонентов ЭВМ последовательного типа: процессор, память, коммуникационная подсистема, периферийные устройства, подсистема обработки прерываний, подсистема прямого доступа к памяти, подсистема энергообеспечения ЭВМ, подсистема охлаждения ЭВМ. Система команд ЭВМ. Способы адресации в ЭВМ.

Тема 3. Организация подсистемы памяти ЭВМ

Основные характеристики памяти ЭВМ. Иерархическая организация памяти ЭВМ. Архитектура статической, динамической, энергонезависимой памяти. Синхронные и асинхронные типы памяти. Способы увеличения быстродействия, разрядности и объемов памяти. Память с ассоциативным доступом. Кэш-память, стратегии размещения и замещения. Архитектура виртуальной памяти.

Тема 4. Организация ввода-вывода в ЭВМ

Общие сведения об организации ввода-вывода в ЭВМ. Шинная организация подсистемы ввода-вывода. Стандарты шин. Интерфейсы периферийных устройств ЭВМ.

Основные типы устройств ввода-вывода. Мониторы. Видео- и звуковые адаптеры. Адаптеры ЛВС. Модемы. Магнитные, оптические и магнитооптические устройства хранения данных. RAID-массивы. Внешние запоминающие устройства на флэш-памяти. Устройства ввода: клавиатура, манипуляторы графической информации, сенсорные экраны графических планшетов и смартфонов, сканеры. Устройства печати: матричные, струйные, лазерные принтеры, плоттеры.

Раздел 2. Архитектура микропроцессорных систем

Тема 5. Современные микропроцессоры

Понятия: архитектура и структура микропроцессора. Принципы функцио-нирования микропроцессора. Классификации микропроцессоров. Основные характеристики микропроцессоров. Особенности микропроцессоров CISC, RISC, VLIW. Способы выявления и использования параллелизма уровня ко-манд. Технологии выполнения команд в микропроцессоре: конвейеризация, ди-намическое выполнение, мультитредовое выполнение. Многоядерные микро-процессоры.

Особенности архитектуры и структуры микропроцессоров: универсальных, сигнальных, сетевых, графических, ввода-вывода, медийные.

Пути совершенствования и перспективные направления развития микропроцессоров.

Тема 6. Микроконтроллеры

Назначение, области применения, архитектура, структура, основные технические характеристики микроконтроллеров. Принципы построения, разработки и отладки микропроцессорных систем на базе микроконтроллеров.

Раздел 3. Архитектура и структура параллельных ВС

Тема 7. Параллельная обработка информации

Типы параллельной обработки и классификация систем параллельной обработки данных. Векторная обработка, понятие о векторизации программ. Конвейерная (магистральная) обработка. Показатели качества и эффективности систем параллельной обработки информации.

Тема 8. Коммуникационные подсистемы параллельных ВС

Архитектуры, структуры и технические характеристики коммуникационных сред параллельных ВС: шинная организация, кольцевые структуры, коммуникационные среды на основе прямоугольных коммутаторов.

Сосредоточенные и распределенные составные коммутаторы, примеры организации. Алгоритмы маршрутизации в составных коммутаторах, способы разрешения тупиковых ситуаций при маршрутизации.

Тема 9. Способы организации параллельных ВС

Векторно-конвейерные, матричные и ассоциативные ВС. Многопроцессорные ВС с общей памятью: симметричный мультипроцессор, системы с неоднородным доступом к памяти; способы обеспечения когерентности памяти. Массово-параллельные, кластерные и гибридные ВС. Параллельные ВС с нетрадиционной архитектурой. Потоковые системы. Систолические и волновые массивы.

Раздел 4. Перспективные направления в развитии ЭВМ и ВС

Тема 10. Технологии построения центров обработки данных

Состав и назначение центров обработки данных (ЦОД). Современные технологии построения ЦОД. Виртуализация аппаратных ресурсов ЦОД, грид-системы, облачные вычислительные инфраструктуры, виды облачных сервисов.

Тема 11. Перспективные направления развития ЭВМ и ВС

Новые направления в развитии вычислительной техники и ее технологической базы. Нанотехнологии. Нейронные, оптические, молекулярные, криогенные, квантовые ЭВМ.

Форма контроля: *2 экзамена, курсовая работа*

Перечень материально-технического обеспечения:

Специфического материально-технического обеспечения не требуется.

*Б.1.О.16 Дисциплина «Сети и системы передачи информации»*

Коды формируемых компетенций: *ОПК-9*

В результате изучения дисциплины студент должен

знать:

* основные характеристики сигналов электросвязи, спектры и виды модуляции;
* способы кодирования информации

уметь:

* анализировать основные характеристики и возможности телекоммуникационных систем

Примерное распределение часов: не менее 180 ч.

Форма контроля: *экзамен*

Содержание дисциплины:

Тема 1. Основы организации и функционирования вычислительных сетей

Понятие вычислительной сети. Этапы развития вычислительных сетей. Классификация вычислительных сетей. Характеристики вычислительных сетей. Средства построения локальных вычислительных сетей (ЛВС). Принципы построения и функционирования локальных и глобальных вычислительных сетей.

Тема 2. Стандартизация вычислительных сетей

Логическая и физическая структуризация вычислительных сетей. Модель ISO/OSI. Стандартные стеки коммуникационных протоколов. Понятие открытой спецификации. Формирование и внедрение открытой спецификации. Сеть Интернет – как пример сети с открытыми спецификациями. Основные протоколы локальных вычислительных сетей.

Тема 3. Физический уровень

Физический уровень построения вычислительных сетей. Виды коммуникационных сред. Линия связи. Характеристики линии связи. Стандарты кабелей, используемых для построения сетей. Структурированная кабельная система. Средства предотвращения несанкционированного доступа к коммуникационной среде. Кодирование цифровой информации. Модуляция сигналов. Мультиплексирование сигналов.

Тема 4. Канальный уровень

Канальный уровень построения вычислительных сетей. Методы доступа к разделяемой среде. Методы коммутации. Защита информации на канальном уровне в ЛВС.

Тема 5. Построение ЛВС

Этапы планирования, проектирования, организации, развертывания и использования ЛВС с учетом требований по обеспечению безопасности. Стандарты построения физического и канального уровня. Стандарты IEEE 802.x. Методы доступа к разделяемой среде. Методы доступа, используемые в сетях Ethernet и WiFi. Форматы кадров технологии Ethernet. Высокоскоростные технологии построения ЛВС. Объединение сегментов сети с использованием коммутаторов. Администрирование коммутаторов. Технологии VLAN.

Тема 6. Сетевой уровень

Сетевой уровень построения вычислительных сетей. Функции и интерфейсы сетевого уровня. Сетевой уровень Internet. Протоколы IPv4, IPv6, адресация в IP-сетях. Протоколы разрешения адресов ARP, RARP. Протокол динамического выделения сетевых настроек (DHCP). Технология NAT.

Тема 7. Маршрутизация в локальных и глобальных вычислительных сетях

Маршрутизация в вычислительных сетях. Статическая маршрутизация. Динамическая маршрутизация. Алгоритмы маршрутизации, их характеристики. Протоколы внутренней и междоменной маршрутизации (RIP, OSPF, IGRP, EGP, BGP). Объединение локальных сетей с использованием маршрутизатора. Администрирование маршрутизатора. Определение и редактирование сетевых настроек.

Рекомендуемый перечень лабораторных работ:

Построение элементов структурированной кабельной системы.

Организация ЛВС с использованием различных коммуникационных сред.

Построение сетей с помощью коммутаторов.

Применение технологии VLAN.

Адресация на сетевом уровне. Протокол IP.

Статическая маршрутизация.

Рекомендуемый перечень основной литературы:

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: учеб. пособие для студентов вузов. 4-е изд. – СПб.: Питер, 2014. – 943 с.
2. Таненбаум Э., Уэзеролл Д. Компьютерные сети; пер. с англ. А. Гребенькова. Изд. 5-е. – СПб.: Питер, 2017. – 955 с.
3. Платонов В.В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей: учеб. пособие для вузов. – М.: Издательский центр «Академия», 2006. – 239 с.
4. Смелянский Р. Л. Компьютерные сети: в 2 т.: учебник. Т. 1: Системы передачи данных. – М.: Издательский центр «Академия», 2011. – 297 с.
5. Смелянский Р. Л. Компьютерные сети: в 2 т.: учеб. для студентов вузов. Т. 2: Сети ЭВМ. – М.: Издательский центр «Академия», 2011. – 240 с.

Перечень материально-технического обеспечения:

1. Установочные пакеты программных средств обеспечения безопасности внешнего периметра сети ЭВМ (SNORT или аналог).
2. Программное средство построения виртуальных машин (VMWare или аналог).
3. Программные сетевые анализаторы (WireShark или аналог).
4. Система программирования с библиотеками Berkley Sockets.
5. Модуль МСЭ для ОС (Iptables или аналог).

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

Коды формируемых компетенций: *ОПК-7*

В результате изучения дисциплины студент должен

знать:

* общие принципы построения, области и особенности применения языков программирования высокого уровня;
* язык программирования высокого уровня (объектно-ориентированное программирование)

уметь:

* работать с интегрированной средой разработки программного обеспечения;
* разрабатывать и реализовывать на языке высокого уровня алгоритмы решения типовых профессиональных задач

Примерное распределение часов: не менее 324 ч.

Форма контроля: *зачет, экзамен*

Содержание дисциплины:

Основы языков программирования высокого уровня. Базовые средства описания данных. Базовые средства описания действий. Структурное программирование. Указатели и массивы. Функции. Стандартная библиотека С. Составные типы данных. Структуры с динамически изменяемыми размерами. Препроцессор. Основы объектно-ориентированного программирования. Средства реализации основных принципов ООП в языке C++. Наследование, полиморфизм. Шаблоны классов. Контейнеры STL. Многопоточность в STL. Шаблоны проектирования. Исключительные ситуации. Динамически подключаемые библиотеки. Конвенции программирования.

Рекомендуемый перечень лабораторных работ:

* Разработка программ на основе циклов.
* Разработка программ с использованием структур данных.
* Работа с динамической памятью в языке С++.
* Работа со строками в языке С++. Библиотечный класс string.

Перечень материально-технического обеспечения:

Специфического материально-технического обеспечения не требуется.

*Б.1.О.18 Дисциплина «Технологии и методы программирования»*

Коды формируемых компетенций: *ОПК-7*

В результате изучения дисциплины студент должен

знать:

* методы тестирования и отладки программного обеспечения;
* современные технологии и методы программирования;
* принципы организации документирования разработки, процесса сопровождения программного обеспечения;
* показатели качества программного обеспечения;

уметь:

* проводить тестирование и отладку программных систем;
* проектировать структуру и архитектуру программного обеспечения с использованием современных методологий и средств автоматизации проектирования программного обеспечения;
* применять известные методы программирования и возможности базового языка программирования для решения типовых профессиональных задач

Примерное распределение часов: не менее 324 ч.

Форма контроля: *зачет, экзамен*

Содержание дисциплины:

Раздел 1. Технологии программирования

Тема 1. Жизненный цикл ПО, методологии и стандарты разработки ПО

Современные технологии и методы программирования. Жизненный цикл ПО. Модели жизненного цикла ПО. Стандарты в сфере разработки ПО. Процессы жизненного цикла ПО. Модель зрелости предприятия. Основные этапы разработки сложных программных систем. Требования и внешние спецификации к ПО. Структура и состав технического задания в соответствии ГОСТ. Этапы разработки ПО в соответствии с ГОСТ. Методологии разработки ПО. Показатели качества ПО.

Тема 2. Планирование и организация разработки ПО

Основы планирования разработки программного обеспечения. Подходы к оценке сложности, времени разработки ПО по показателям качества. Размерно- и функционально-ориентированные метрики оценки сложности и времени разработки ПО. Конструктивная модель оценки ПО.

Принципы организации разработки ПО. Методологии и методы проектирования ПО. Организация коллективов разработчиков ПО. Функции и роли разработчиков в программных проектах, совмещение ролей в рамках одного проекта. Средства поддержки планирования и контроля процесса разработки ПО. Методологии планирования и организации разработки ПО.

Тема 3. Проектирование ПО

Требования к программному продукту: определения, характеристики требований, типы требований, способы организации взаимодействия разработчика и заказчика. Требования надежности, безопасности, защищенности. Стандарты в сфере формирования требований к программному обеспечению. Способы извлечения требований.

Внешнее проектирование программного обеспечения. Внешние спецификация небольших программ и программных модулей. Методы и средства внешнего проектирования. Структурное проектирование ПО – основные принципы, понятие структурной декомпозиции.

CASE-технологии. Методология структурного анализа и проектирования (SADT). Моделирование потоков данных (DFD). Критерии завершения проектирования.

Понятия архитектуры и структуры ПО. Проектирование архитектуры и структуры ПО. Требования к качественной архитектуре, характеристики качества архитектуры и структуры ПО. Виды программных архитектур. Образцы проектирования архитектур, архитектурные стили. Метрики оценки качества некоторых архитектур. Проверка качества архитектуры.

Проектирование интерфейса ПО. Виды пользовательских интерфейсов (ПИ). Вопросы стандартизации ПИ. Факторы удобства использования интерфейса. Механизмы обеспечения понятности ПИ, принцип концептуальной целостности. Методы разработки удобного интерфейса. Методы оценки качества ПИ.

Тема 4. Основы объектно-ориентированного анализа и проектирования ПО

Некоторые ограничения структурных методологий. Объектно-ориентированные анализ (ООА) и проектирование (ООП) структуры и архитектуры ПО. Основные понятия ООА и ООП. Объектная декомпозиция. Нотации ООА и ООП. UML – цели создания, история развития, преимущества в области разработки программных систем. Нотация UML. Расширения UML.

Тема 5. Кодирование ПО

Общее содержание этапа кодирования ПО. Структурное программирование. Преимущества структурированных алгоритмов и программ. Метод «пошаговой детализации» при проектировании структурированных программ. Стиль программирования как набор традиционных правил оформления текста программы. Элементы качественного стиля программирования. Вопросы стандартизации стилей программирования. Понятие защитного программирования. Написание надежного кода с использованием приемов защитного программирования.

Тема 6. Тестирование и отладка ПО

Понятия программной ошибки и надежность программного обеспечения. Общие подходы к предупреждению, выявлению и нейтрализации факторов, снижающих надежность программного обеспечения. Причины и источники ошибок в программах.

Понятие тестирования, виды и этапы тестирования. Верификация и валидация. Методы тестирования программ вручную. Критерии тестирования. Стратегии проектирования тестов, методы эквивалентных разбиений, граничных значений, таблиц решений, функциональных диаграмм, предположений об ошибке, методы покрытия логики. Основы комплексного применения методов проектирования тестов, планы тестирования и списки тестов. Виды программных документов, разрабатываемых на этапе тестирования ПО.

Тестирование модулей: автономное тестирование, методы “пошагового” тестирования. Интеграционное тестирование. Специфика тестирования объектно-ориентированных программ. Регрессионное тестирование. Методы проектирования регрессионных тестов.

Этапы отладки программного обеспечения. Локализация ошибок. Аналитические и экспериментальные методы отладки программ. Общая характеристика современных средств отладки. Исправление ошибок в программе. Анализ результатов отладки. Специфика отладки систем реального времени.

Тема 7. Документирование ПО

Виды программной документации. Общие принципы составления качественной документации для пользователя программы и организации документирования разработки ПО, порядок составления и возможные способы представления документации. Единая система программной документации (ЕСПД), назначение и состав. Автоматизированное документирование ПО с использованием интегрированных сред разработки ПО.

Тема 8. Сопровождение ПО

Задачи сопровождения программного обеспечения. Основные направления повышения качества фаз эксплуатации и сопровождения программного обеспечения, подготовка условий для качественного проектирования последующих версий программы. Организация процесса сопровождения ПО. Инструментальные средства поддержки сопровождения программных систем. Порядок внесения изменений в программное обеспечение и управление версиями программы. Средства управления версиями ПО.

Тема 9. Перспективы развития технологий программирования

Перспективы развития технологий и методов программирования с учетом средств автоматизации процессов проектирования, создания и тестирования программного обеспечения: системы управления проектами, системы контроля версий, средства автоматизации документирования и тестирования ПО.

Раздел 2. Методы программирования

Тема 10. Методы анализа алгоритмов

Методы программирования по оценке сложности алгоритмов. Наихудшие и средние показатели, порядок роста сложности алгоритма. Способы оценки сложности алгоритмов. Методы анализа рекурсивных алгоритмов. Методы построения и анализа алгоритмов (динамическое программирование, амортизационный анализ, жадные алгоритмы). Выбор способа реализации алгоритмов их тестирование и отладка в интегрированной среде разработки ПО.

Тема 11. Динамические структуры данных

Методы программирования с использованием структур данных: множества, списки, стеки, очереди, деревья, «кучи», хеш-таблицы. Способы реализации структур данных и основные операции над ними. Выбор способа реализации алгоритмов их тестирование и отладка в интегрированной среде разработки ПО.

Тема 12. Поиск и сортировка

Основные комбинаторные алгоритмы, способы их реализации и оценки сложности. Алгоритмы сортировки последовательностей (слиянием, вставками, быстрая сортировка, сортировки сравнением). Алгоритмы поиска (линейный, двоичный, Фибоначчи; деревья поиска). Поиск в хеш-таблице.Алгоритмы поиска в строке (алгоритмы Бойера-Мура, Пратта). Алгоритмы определения расстояния для строк (алгоритм Левенштейна, алгоритм Фишера). Выбор способа реализации алгоритмов их тестирование и отладка в интегрированной среде разработки ПО.

Тема 13. Основные алгоритмы на графах

Методы программирования с использованием представления данных в виде графов. Основные теоретико-графовые алгоритмы, способы их реализации и оценки сложности. Алгоритмы обхода графов. Алгоритмы нахождения сильносвязных компонент, минимальных остовных деревьев, кратчайших путей, максимального потока. Топологическая сортировка, задача коммивояжера, приближенные алгоритмы. Выбор способа реализации алгоритмов их тестирование и отладка в интегрированной среде разработки ПО.

Рекомендуемый перечень основной литературы:

1. Анашкина, Н. В. Технологии и методы программирования: учеб. пособие для студентов вузов / Н. В. Анашкина, Н. Н. Петухова, В. Ю. Смольянинов. - М. : Издательский центр «Академия», 2012. - 378 с.
2. Кулямин В.В. Технологии программирования. Компонентный подход. Учебное пособие. Москва: Интернет-Университет Информационных Технологий (ИНТУИТ) . 2016 - 590 с. ISBN: 5-9556-0067-1 (ЭБС IPRbooks) .
3. Алгоритмы: построение и анализ / Т. Кормен ; кол. авт.: Т. Кормен [и др.] ; пер. с англ. и ред. И. В. Красикова. - 3-е изд. - М. : Вильямс, 2014. - 1323 с.
4. Калентьев А.А., Гарайс Д.В., Горяинов А.Е. Новые технологии в программировании. Учебное пособие. Томск: Томский государственный университет систем управления и радиоэлектроники, Эль Контент 2014 – 176 с. ISBN: 978-5-4332-0185-9 (ЭБС IPRbooks).
5. Назаренко П.А. Алгоритмы и структуры данных Учебное пособие. Самара: Поволжский государственный университет телекоммуникаций и информатики 2015 - 130 с. (ЭБС IPRbooks).

Перечень материально-технического обеспечения:

Специфического материально-технического обеспечения не требуется.

*Б.1.О.19 Дисциплина «Безопасность операционных систем»*

Коды формируемых компетенций: *ОПК-10, ОПК-12, ОПК-15*

В результате изучения дисциплины студент должен

знать:

* принципы организации и структуру систем защиты информации современных операционных систем;
* критерии оценки эффективности и надежности систем защиты информации операционных систем;
* принципы построения и функционирования, примеры реализаций современных операционных систем;
* принципы организации и структуру систем защиты информации современных операционных систем

уметь:

* конфигурировать параметры системы защиты информации современных операционных систем;
* контролировать эффективность принятых мер по реализации политик безопасности информации в современных операционных системах;
* оценивать эффективность и надежность защиты операционных систем;
* проводить установку и настройку современных операционных систем с учетом требований по обеспечению информационной безопасности;
* использовать средства операционных систем для обеспечения безопасного функционирования автоматизированных систем;
* восстанавливать операционные системы после сбоев

Примерное распределение часов: не менее 360 ч.

Форма контроля: *зачет, экзамен*

Содержание дисциплины:

История развития компьютеров и операционных систем. Загрузка ОС. Файловые системы. Взаимодействие ОС с пользователей, командные файлы. Операционные среды. Драйверы. Планирование и диспетчеризация. Управление памятью. Управление устройствами и вводом/выводом. Модели управления доступом к информации и политики безопасности. Требования к защите ОС. Модели безопасности основных ОС. Системы защиты программного обеспечения. Виртуальные машины. Авторизация и аутентификация. Руткит. Протоколирование и аудит.

Рекомендуемый перечень лабораторных работ:

1. Использование скриптов.
2. Настройка разграничений доступа штатными средствами ОС.
3. Системы защиты программного обеспечения.
4. Использование виртуальных машин.
5. Настройка авторизации и аутентификации пользователей ОС.
6. Конфигурирование систем протоколирования и аудита.
7. Проскурин В. Г. Защита в операционных системах : учеб. пособие для студентов вузов / - М. : Горячая линия-Телеком, 2014. - 192 с.
8. Дейтел Х. М., Дейтел П. Дж., Чофнес Д. Р.  Операционные системы. Т.1: Основы и принципы /; пер. с англ. под ред. А. С. Молявко. - 3-е изд. - М.: БИНОМ, 2011. - 1023 с.
9. Дейтел Х. М., Дейтел П. Дж., Чофнес Д. Р. Операционные системы . Т. 2: Распределённые системы, сети, безопасность / ; пер. с англ. под ред. А.С.Молявко. - 3-е изд. - М. : БИНОМ, 2011. - 704 с.

Перечень материально-технического обеспечения:

Специфического материально-технического обеспечения не требуется.

*Б.1.О.20 Дисциплина «Безопасность вычислительных сетей»*

Коды формируемых компетенций: *ОПК-10, ОПК-12, ОПК-15*

В результате изучения дисциплины студент должен

знать:

* основные протоколы, используемые для защиты информации в вычислительных сетях;
* основные криптографические методы, используемые для защиты информации в вычислительных сетях;
* принципы построения и функционирования локальных и глобальных вычислительных сет

уметь:

* проводить анализ угроз безопасности в локальных вычислительных сетях;
* реализовывать политику безопасности в локальной вычислительной сети

Примерное распределение часов: не менее 360 ч.

Форма контроля: *зачет, экзамен*

Содержание дисциплины:

Тема 1. Транспортная подсистема вычислительных сетей

Транспортный уровень построения вычислительных сетей. Транспортные протоколы в Internet: TCP и UDP. Интерфейс Berkley Sockets. Угрозы безопасности и средства организации безопасного информационного взаимодействия в сетях TCP/IP.

Тема 2. Уровень приложений

Представительский и прикладной уровни построения вычислительных сетей. Протоколы прикладного и представительского уровней сети Internet. Система DNS. Администрирование служб доменных имен.

Тема 3. Службы локальных вычислительных сетей

Модель «клиент-сервер». Виды серверов и протоколы взаимодействия (HTTP, FTP, SMTP, RDP, SSH и другие). Основные сетевые службы прикладного уровня. Службы файлового обмена. Службы веб-серверов и электронной почты. Служба каталогов Active Directory. Политика безопасности и групповые политики. Решение задач администрирования Active Directory на базе ОС Windows Server. Решение задач администрирования веб-сервера, служб файлового обмена, сервера электронной почты, сервера баз данных.

Тема 4. Алгоритмы криптографической защиты информации в ЛВС

Основные криптографические методы, используемые для защиты информации в вычислительных сетях. Понятие аутентификации. Виды аутентификации. Виды шифрования. Основные протоколы, используемые для защиты информации в вычислительных сетях. Протоколы аутентификации и шифрования с открытым ключом. Организация защищенного канала связи с использованием криптографических протоколов. Виртуальные частные сети. Протокол SSL.

Тема 5. Анализ защищенности ЛВС

Методы и средства защиты информации в локальных вычислительных сетях. Понятие сетевая атака. Классификация сетевых атак. Виды сетевых атак и методы их реализации. Анализ защищенности и угроз безопасности ЛВС. Сетевое сканирование. Администрирование средств сетевого сканирования и реализации сетевых атак.

Тема 6. Средства контроля сетевого трафика в ЛВС

Политика безопасности в локальной вычислительной сети. Понятие межсетевого экрана (МСЭ). Функции МСЭ. Классификация МСЭ. Способы реализации МСЭ. Модуль IPTABLES как средство реализации МСЭ. Настройка IPTABLES для решения задач фильтрации и блокирования сетевого трафика. Средства контроля доступа к сетевым службам.

Тема 7. Средства обнаружения вторжений в ЛВС

Классификация средств обнаружения вторжений (СОВ). Способы реализации СОВ. Сетевой анализатор Wireshark. Анализ сетевого трафика и угроз безопасности в ЛВС. Современные программно-аппаратные СОВ. Средства обеспечения безопасности внешнего периметра ЛВС (на примере модуля SNORT).

Тема 8. Безопасность в ЛВС

Особенности эксплуатации локальных вычислительных сетей с учетом требований по обеспечению безопасности. Средства организации ложного информационного ресурса в ЛВС. Использование средств защиты информации в ЛВС с учетом требований по обеспечению безопасности. Защита информации в ЛВС на разных уровнях: физическом, канальном, сетевом, прикладном. Средства обнаружения несанкционированного доступа к информации на разных уровнях ЛВС. Администрирование ЛВС с учетом требований по обеспечению безопасности.

Рекомендуемый перечень лабораторных работ:

Построение элементов структурированной кабельной системы.

Построение сетей с помощью коммутаторов. Применение технологии VLAN.

Анализ протоколов взаимодействия клиент-серверного приложения с использованием сокетов.

Применение протокола SNMP.

Организация VPN.

Конфигурирование средств обнаружения вторжений.

Перечень материально-технического обеспечения:

1. Установочные пакеты программных средств обеспечения безопасности внешнего периметра сети ЭВМ (SNORT или аналог).
2. Программное средство построения виртуальных машин (VMWare или аналог).
3. Программные сетевые анализаторы (WireShark или аналог).
4. Система программирования с библиотеками Berkley Sockets.
5. Модуль МСЭ для ОС (Iptables или аналог).

*Б.1.О.21 Дисциплина «Безопасность систем баз данных»*

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

В результате изучения дисциплины студент должен

знать:

* принципы построения и функционирования, примеры реализаций современных систем управления базами данных;
* средства защиты информации систем управления базами данных

уметь:

* разрабатывать и администрировать базы данных;
* конфигурировать средства защиты информации систем управления базами данных

Примерное распределение часов: не менее 360 ч.

Форма контроля: *зачет, экзамен*

Содержание дисциплины:

Назначение и роль систем баз данных. Основы теории баз данных. Реляционные базы данных. Проектирование баз данных. Физическая организация баз данных. Средства поддержания интерфейса с различными категориями пользователей. Средства обеспечения безопасности данных. Архитектура СУБД. Организация доступа к данным в СУБД. Защита информации в СУБД. Угрозы информационной безопасности баз данных. Политика безопасности БД. Средства обеспечения информационной безопасности в СУБД. Аудит систем баз данных.

Рекомендуемый перечень лабораторных работ:

* Модификация данных.
* Выборка данных.
* Проектирование разграничения доступа.
* Настройка разграничения доступа.
* Управление одновременным доступом к данным в СУБД.
* Обеспечение целостности данных с помощью механизма транзакций.

Перечень материально-технического обеспечения:

Специфического материально-технического обеспечения не требуется.

*Б.1.О.22 Дисциплина «Основы информационной безопасности»*

Коды формируемых компетенций: *ОПК-1*

В результате изучения дисциплины студент должен

знать:

* сущность и понятие информации, информационной безопасности и характеристику ее составляющих;
* место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики;
* источники и классификацию угроз информационной безопасности;
* основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;
* основные понятия, связанные с обеспечением информационной безопасности личности, общества и государства, понятия информационного противоборства, информационной войны и формы их проявлений в современном мире

уметь:

* классифицировать и оценивать угрозы информационной безопасности.

Примерное распределение часов: не менее 108 ч.

Форма контроля: *зачет*

Содержание дисциплины:

Модели нарушителя. Вредоносное программное обеспечение. Средства защиты информации. Вывод АС из эксплуатации. Компьютерно-техническая экспертиза. Информационное противоборство. Защита информации от утечки по техническим каналам.

Перечень материально-технического обеспечения:

Специфического материально-технического обеспечения не требуется.

*Б.1.О.23 Дисциплина «Организационное и правовое обеспечение информационной безопасности»*

Коды формируемых компетенций: *ОПК-5, ОПК-6, ОПК-14*

В результате изучения дисциплины студент должен

знать:

* основные угрозы безопасности информации и модели нарушителя в автоматизированных системах;
* основы: российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федераци

уметь:

* обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав;
* анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации;
* формулировать основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации;
* формулировать основные требования информационной безопасности при эксплуатации автоматизированной системы;
* формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации

Примерное распределение часов: не менее 180 ч.

Форма контроля: *экзамен*

Содержание дисциплины:

Правовая система Российской Федерации. Информация как объекта права. Обеспечение безопасности информации и компетенция органов государственной власти по обеспечению информационной безопасности. Федеральные и ведомственные нормативные акты в области ИБ. Международные и отечественные стандарты в сфере ИБ. Лицензирование, сертификация и аттестация в сфере ИБ.

Перечень материально-технического обеспечения:

Специфического материально-технического обеспечения не требуется.

*Б.1.О.24 Дисциплина «Защита информации от утечки по техническим каналам»*

Коды формируемых компетенций: *ОПК-5, ОПК-6, ОПК-13*

В результате изучения дисциплины студент должен

знать:

* способы и средства контроля эффективности защиты информации;
* способы и средства защиты информации от утечки по техническим каналам;
* технические каналы утечки информации;
* нормативные документы в области технической защиты информации;
* нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа;
* основные угрозы безопасности информации и модели нарушителя объекта информатизации

уметь:

* использовать средства инструментального контроля показателей эффективности технической защиты информации;
* разрабатывать модели угроз и модели нарушителя объекта информатизации;
* разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации;
* определить политику контроля доступа работников к информации ограниченного доступа;
* формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации

Примерное распределение часов: не менее 180 ч.

Форма контроля: *экзамен*

Содержание дисциплины:

Цели и задачи защиты информации от утечки информации по техническим каналам. Электромагнитные технические каналы утечки информации, обрабатываемой средствами вычислительной техники (СВТ). Технические каналы утечки акустической (речевой) информации. Способы и средства защиты объектов информатизации от утечки информации по техническим каналам. Способы и средства защиты выделенных помещений от утечки речевой информации по техническим каналам. Методы и средства контроля защищенности информации, обрабатываемой СВТ. Методы и средства контроля защищенности речевой информации от утечки по техническим каналам.

Перечень материально-технического обеспечения:

Специфического материально-технического обеспечения не требуется.

*Б.1.О.25 Дисциплина «Методы и средства криптографической защиты информации»*

Коды формируемых компетенций: *ОПК-10*

В результате изучения дисциплины студент должен

знать:

* основные задачи и понятия криптографии;
* модели шифров и математические методы их исследования

уметь:

* применять математические методы исследования моделей шифров;
* использовать типовые криптографические алгоритмы

Примерное распределение часов: не менее 180 ч.

Форма контроля: *экзамен*

Содержание дисциплины:

Место криптографических методов в защите информации. Угрозы информации и задачи ее защиты. Алгебраическая модель шифра. Математические модели простейших шифров. Понятие о шифрах замены и перестановки, блочных и поточных шифрах. Основные требования к шифрам в связи с возможными угрозами к защищаемой информации. Одноалфавитные шифры замены. Одноалфавитные шифры. Математическое описание и методы криптоанализа шифрсистем однобуквенной простой замены, равнозначной простой замены, разнозначной замены, пропорциональных шифров. Формальные модели открытого текста. Частотные характеристики открытых текстов, критерии распознавания открытого текста (критерий Неймана-Пирсона, критерий запретных биграмм, критерий для форматированных текстов). Методы криптоанализа, основанные на вероятных словах и шаблонах. Ключевые системы шифров замены. Методы конструирования алфавитных подстановок: по ключевому слову (лозунгу), по таблице, по книге. Методы предварительной подготовки открытых текстов для зашифрования. Устранение избыточности открытых текстов, сжатие открытых текстов, перешифровка. Шифры перестановки. Математическое описание и методы криптоанализа шифров горизонтальной перестановки, вертикальной перестановки, решетки Кардано на основе частотных свойств биграмм естественного языка. Методы криптоанализа шифров замены и перестановки на основе эвристических алгоритмов. Многоалфавитные шифры. Исторический очерк, математическое описание и методы криптоанализа многоалфавитных шифрсистем: диска Альберти, шифра Виженера, шифра Бофорта, таблицы Тритемия. Ключевые системы многоалфавитных шифрсистем. Математический аппарат криптоанализа многоалфавитных шифров. Тест Казизски. Индексы совпадения Фридмана и другие тесты Фридмана. Методы криптоанализа на основе эвристических алгоритмов поиска Баума, Якобсена, генетических алгоритмов, алгоритма муравьиной колонии и алгоритма имитации отжига. Криптоанализ шифров гаммирования в случаях использования неравновероятной гаммы или повторного использования гаммы. Биграммные шифры. Математическое описание и методы криптоанализа шифрсистем «шифр Плейфера» и «шифр Хилла». Понятие о композиционных шифрах. Разделенный шифр Чейза. Шифровальные машины. Исторический очерк, математическое описание и принципы криптоанализа шифрмашин М-209 и «Энигма». Ключевые системы, их достоинства и слабости, предварительное распределение ключей и способы выработки разового ключа. Методы подготовки открытого текста для зашифрования. Использование композиционных шифров. Методы полного перебора ключей и особенности их реализации. Бомба Тьюринга. Эвристический метод криптоанализа трехдискового шифратора. Электронные шифраторы. Математическое описание базовых блочных алгоритмов зашифрования DES и ГОСТ 28147 89. Реализация поточных шифрсистем с помощью блочных шифров. Описание стандартных режимов шифрования и сравнение показателей помехоустойчивости для них. Задачи противостояния случайным и целенаправленным помехам. Криптоанализ трехраундовых шифров DES-3 и ГОСТ-3. Защита информации с помощью криптосистем с открытым ключом. Понятие однонаправленной функции с секретом (ОФС). Примеры кандидатов на ОФС. Понятие о системе шифрования с открытым ключом. Криптосистема RSA. Задачи защиты информации, решаемые с помощью ОФС: обеспечение конфиденциальности, аутентичности сообщения и отправителя, доказательство авторства и другие. Понятие криптографической хеш-функции. Понятие криптографического протокола. Простейшие криптографические протоколы, использующие асиммет¬ричное шифрование. Основные методы распределения ключей. Предварительное распределение ключей. Пересылка ключей. Открытое распределение ключей. Схема разделения секрета. Теоретическая стойкость шифров. Алгебраические и вероятностные модели шифров. Основные требования к шифрам. Характеристики вероятностной модели шифра. Совершенные шифры. Теорема К. Шеннона о минимальных совершенных шифрах. Понятие ложных ключей и расстояния единственности. Практическая стойкость шифров. Криптоатаки. Понятие практически стойкого шифра. Методы перебора ключей. Параметры тотального перебора ключей. Методы определения ключей, использующие память. Метод Хеллмана. Методы линеаризации систем нелинейных уравнений. Псевдослучайные функции и доказуемая стойкость криптосистем. Случайные и псевдослучайные функции и подстановки. Понятие доказуемой стойкости в терминах вероятностной неотличимости. Оценка стойкости режимов блочного шифрования. Имитостойкость шифров. Понятие имитостойкого шифра. Вероятности успеха активных атак при навязывании наугад. Оценки параметров имитостойкости шифра. Примеры имитовставок.

Перечень материально-технического обеспечения:

Специфического материально-технического обеспечения не требуется.

*Б.1.О.26 Дисциплина «Программно-аппаратные средства защиты информации»*

Коды формируемых компетенций: *ОПК-9*

В результате изучения дисциплины студент должен

знать:

* текущее состояние и тенденции развития методов и средств защиты информации в операционных системах, съемных носителях и сетях передачи данных;
* принципы построения и особенности функционирования систем контроля и управления доступом в автоматизированных системах;;
* подходы к анализу защищенности компонентов автоматизированных систем и поиску потенциальных уязвимостей безопасности информации

уметь:

* анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах

Примерное распределение часов: не менее 216 ч.

Форма контроля: *экзамен*

Содержание дисциплины:

Назначение и функции программно-аппаратных средств защиты информации. Методы защиты информации от несанкционированного доступа. Аппаратные компоненты систем защиты информации автоматизированных систем. Средства обеспечения информационной безопасности вычислительных сетей. Комплексное обеспечение информационной безопасности автоматизированных систем.

Рекомендуемый перечень лабораторных работ:

* Применение средств шифрования данных.
* Генерация ключей шифрования.
* Настройка механизма сертификации.
* Защита данных передаваемых по сети.
* Настройка защищенного удаленного доступа к системе управления базами данных.

Перечень материально-технического обеспечения:

Специфического материально-технического обеспечения не требуется.

*Б.1.О.27 Дисциплина «Управление информационной безопасностью»*

Коды формируемых компетенций: *ОПК-5, ОПК-15*

В результате изучения дисциплины студент должен

знать:

* программные средства, позволяющие вести автоматизированный аудит;
* основные документы по стандартизации в сфере управления ИБ;
* принципы формирования политики информационной безопасности в автоматизированных системах;
* требования информационной безопасности при эксплуатации автоматизированной системы

уметь:

* осуществлять выбор и обоснование критериев эффективности функционирования защищенных автоматизированных информационных систем;
* разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы;
* формировать политики информационной безопасности организации;
* выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы

Примерное распределение часов: не менее 180 ч.

Форма контроля: *экзамен*

Содержание дисциплины:

Система управления информационной безопасностью (ИБ) автоматизированных систем (АС). Системный подход к проектированию, внедрению и поддержанию системы обеспечения ИБ в организации. Стандартизация в сфере управления ИБ. Политика безопасности предприятия и автоматизированных систем. Модель нарушителя политики безопасности. Типичные угрозы информации и уязвимости корпоративных АС. Разграничение полномочий и ответственности персонала, обеспечивающего реализацию положений нормативно-распорядительных документов по защите информации организации. Аудит информационной безопасности автоматизированных систем. Стандартизация в сфере аудита ИБ. Содержание и организация процесса аудита ИБ. Оценка рисков ИБ. Отчетные документы по результатам аудита. Выполнение рекомендаций по итогам проведения аудита ИБ.

Перечень материально-технического обеспечения:

Специфического материально-технического обеспечения не требуется.

*Б.1.О.28 Дисциплина «Разработка и эксплуатация автоматизированных систем в защищенном исполнении»*

Коды формируемых компетенций: *ОПК-11, ОПК-13, ОПК-14*

В результате изучения дисциплины студент должен

знать:

* методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем;
* методы, способы, средства, последовательность и содержание этапов разработки систем защиты информационной автоматизированных систем;
* методы, способы и средства обеспечения отказоустойчивости автоматизированных систем;
* основные угрозы безопасности информации и модели нарушителя в автоматизированных системах;
* содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации;
* критерии оценки эффективности и надежности средств защиты информации программного обеспечения автоматизированных систем

уметь:

* проектировать защищенные автоматизированные системы с учетом действующих нормативных и методических документов;
* разрабатывать техническую документацию на компоненты автоматизированных систем;
* осуществлять контроль обеспечения уровня защищенности в автоматизированных системах;
* обнаруживать и устранять нарушения правил разграничения доступа в автоматизированных системах;
* определять источники и причины возникновения инцидентов безопасности в автоматизированных системах;
* контролировать события безопасности и действия пользователей автоматизированных систем;
* контролировать эффективность принятых мер по реализации политик безопасности информации автоматизированных систем;
* документировать процедуры и результаты контроля функционирования системы защиты информации автоматизированной системы;
* осуществлять планирование и организацию работы персонала автоматизированной системы с учетом требований по защите информации;
* определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем

Примерное распределение часов: не менее 216 ч.

Форма контроля: *экзамен*

Содержание дисциплины:

Защищенные автоматизированные системы. Основные понятия и классификация. Основы организации разработки защищенных АС. Общие принципы проектирования защищенных АС. Основы эксплуатации защищенных АС. Аттестация АС по требованиям безопасности. Содержание основных документов, определяющих цели, задачи, порядок проведения аттестации. Особенности эксплуатации АС на объекте защиты. Требования и рекомендации по защите государственной тайны и персональных данных при работе АС. Порядок обеспечения защиты информации при эксплуатации АС. Организация технического обслуживания защищенных АС. Средства диагностирования защищенных АС. Аппаратно-программные средства диагностики АС. Аппаратно-программные средства контроля функционирования отдельных элементов, узлов, блоков. Основы администрирования АС. Задачи администрирования подсистем АС. Взаимодействие подсистем АС. Средства администрирования АС. Настройка сетевой подсистемы защищенной АС. Принципы функционирования информационных сервисов АС. Установка и настройка работы информационных сервисов АС. Удаленное администрирование компонентов АС. Управление дисковой подсистемой АС.

Рекомендуемый перечень лабораторных работ:

* Технология создания отказоустойчивых АС.
* Настройка сетевой подсистемы защищенной АС.
* Настройка программных средств администрирования АС.
* Управление дисковой подсистемой АС.

Перечень материально-технического обеспечения:

Специфического материально-технического обеспечения не требуется.

*Б.1.С.4.1 Дисциплина «Информационная безопасность автоматизированных систем критически важных объектов»*

Коды формируемых компетенций: *ОПК-4.1*

В результате изучения дисциплины студент должен

знать:

* порядок разработки технических регламентов для проведения аттестации объектов информатизации по требованиям безопасности информации на критически важных объектах;
* нормативно-методическую базу, регламентирующую деятельность критически важных объектов и обеспечение их информационной безопасности

уметь:

* применять нормативную базу, регламентирующую деятельность критически важных объектов и обеспечение их информационной безопасности;
* разрабатывать технические регламенты для проведения аттестации объектов информатизации по требованиям безопасности информации на критически важных объектах

владеть:

* методиками разработки технических регла- ментов для испытаний объектов информатизации на соответствие требованиям по защите информации автоматизированных систем критически важных объектов;
* навыками настройки средств обеспечения информационной безопасности автоматизированных систем критически важных объектов

Примерное распределение часов: не менее 216 ч.

Форма контроля: *экзамен*

Содержание дисциплины:

Характеристика и параметры критически важных объектов как объектов защиты от технических разведок (объектов КТК). Анализ и оценка разведобстановки в районах расположения типовых критически важных объектов. Организация и осуществление комплексного противодействия техническим разведкам на типовых критически важных объектах. Сертификация средств обеспечения информационной безопасности критически важных объектов и их автоматизированных систем.

Рекомендуемый перечень основной литературы:

1. Основы построения средств и комплексов обеспечения информационной безопасности. [Электронный ресурс]: Электронное учебное пособие (260 Мб). – Воронеж: ВУНЦ ВВС ВВА, 2021 г.

2. Рембовский А.М., Ашихмин А.В., Козьмин В.А. Радиомониторинг: задачи, методы, средства / Под редакцией А.М. Рембовского. – М.: Горячая линия – Теле-ком, 2006. 493 с.

Перечень материально-технического обеспечения:

Специфического материально-технического обеспечения не требуется.

*Б.1.С.4.2 Дисциплина «Мониторинг информационной безопасности критически важных объектов»*

Коды формируемых компетенций: *ОПК-4.2, ОПК-4.3*

В результате изучения дисциплины студент должен

знать:

* методы проведения технических регламентов по обеспечению информационной безопасности критически важных объектов и их автоматизированных систем;
* методы измерения частотных и времен-ных параметров сигнальных демаскирующих признаков объектов мониторинга;
* алгоритмы измерения несущей частоты сигнала и частоты его побочных и внепо-лосных излучений;
* алгоритмы измерения ширины спектра сигнала;
* законы изменения или модуляции несу-щей частоты сигнала;
* порядок определения количества излуча-емых фиксированных частот и величины разноса между ними

уметь:

* вести мониторинг информационной безопасности критически важных объектов;
* проводить измерения частотных парамет-ров сигнальных демаскирующих признаков объектов мониторинга;
* применять современные средства и ком-плексы радио и радиотехнического кон-троля для измерения частотных параметров сигналов

Примерное распределение часов: не менее 180 ч.

Форма контроля: *экзамен*

Содержание дисциплины:

Методы измерения частотных параметров сигналов. Методы измерения временных параметров сигналов. Методы классификации источников радиоизлучения. Методы контроля и идентификации источников радиоизлучения с различны-ми видами сигналов. Измерения параметров объектов мониторинга с использованием современных средств радио и радиотехнического контроля.

Рекомендуемый перечень основной литературы:

1. 1. Мониторинг информационной безопасности критически важных объектов. [Электронный ресурс]: Электронное учебное пособие (260 Мб). – Воронеж: ВУНЦ ВВС ВВА, 2021 г.

2. Раушер К., Йанссен Ф., Минихольд Р. Основы спектрального анализа: Пер. с англ. С.М. Смольского / Под редакцией Ю.А. Гребенко – М.: Горячая линия-Телеком, 2006. – 224 с.

Перечень материально-технического обеспечения:

Специфического материально-технического обеспечения не требуется.

*Б.1.С.4.3 Дисциплина «Основы построения средств и комплексов обеспечения информационной безопасности»*

Коды формируемых компетенций: *ОПК-4.3*

В результате изучения дисциплины студент должен

знать:

* методы измерения частотных и временных параметров сигнальных демаскирующих признаков объектов мониторинга;
* алгоритмы измерения несущей частоты сигнала и частоты его побочных и внеполосных излучений;
* алгоритмы измерения ширины спектра сигнала;
* законы изменения или модуляции несущей частоты сигнала;
* порядок определения количества излучаемых фиксированных частот и величины разноса между ними

уметь:

* проводить измерения частотных параметров сигнальных демаскирующих признаков объектов мониторинга;;
* применять современные средства и комплексы радио и радиотехнического контроля для измерения частотных параметров сигналов.

Примерное распределение часов: не менее 144 ч.

Форма контроля: *зачет с оценкой*

Содержание дисциплины:

Поиск, обнаружение и наблюдение сигналов специальных радиоэлектронных средств комплексами и средствами радио и радиотехнического контроля. Радиопеленгование и местоопределение специальных радиоэлектронных средств в средствах радио и радиотехнического контроля. Основы технического анализа сигналов радиоэлектронных средств. Основы построения и функционирования комплексов радио и радиотехнического контроля.

Рекомендуемый перечень основной литературы:

1. Федеральный закон № 118 от 26 июля 2017 г. «О безопасности критиче-ской информационной инфраструктуры РФ».

2. Волков А.В., Кравцов Е.В., Кущев С.С., Рюмшин Р.И., Серебряков М.А. Теоретические основы технических разведок. Учебное пособие. – Воронеж: ВУНЦ ВВС «ВВА». 2017. – 307 с.

3. Самойлин Е.А. Организация и осуществление комплексного противодей-ствия техническим разведкам. Учебное пособие. – Воронеж: ВУНЦ ВВС «ВВА». 2018. – 343 с.

Перечень материально-технического обеспечения:

Специфического материально-технического обеспечения не требуется.

*Б.1.С.5.1 Дисциплина «Криптографические протоколы и стандарты»*

Коды формируемых компетенций: *ОПК-5.1*

В результате изучения дисциплины студент должен

знать:

* основные криптографические протоколы и стандарты;
* критерии оценки и контроля эффективности используемых криптографических протоколов и стандартов;

уметь:

* выбирать криптографические протоколы и стандарты, для обеспечения информационной безопасности открытых информационных систем;
* осуществлять контроль эффективности средств защиты, реализующих используемые криптографические протоколы и стандарты;

Примерное распределение часов: не менее 216 ч.

Форма контроля: *экзамен*

Содержание дисциплины:

Математические основы и принципы построения спецификаций криптографических алгоритмов. Этапы развития зарубежных криптографических стандартов. Стандарты DES, AES, DSS. Стандарты ГОСТ 28147 – 89, P 34.10-94, P 34.11-94. Стандарты ГОСТ P 34.10-2001, P 34.11-2001, P 34.10-2012, P 34.11-2012, P 34.12-2015, P 34.13-2015. Методические рекомендации технического комитета ТК26. Перспективные направления развития криптографических стандартов. Классификация криптографических протоколов. Области применения. Вопросы стандартизации, поддержки и совместимости криптографических протоколов.

Рекомендуемый перечень лабораторных работ:

Выбор и использование библиотек длинночисленных типов данных для реализации криптографических преобразований;

Программная реализация компонентов блочного шифра «Магма» ГОСТ Р 34.12-2015;

Программная реализация компонентов блочного шифра «Кузнечик» ГОСТ Р 34.12-2015;

Программная реализация режимов шифрования по ГОСТ Р 34.13-2015;

Программная реализация компонентов функции хеширования ГОСТ Р 34.11-94;

Программная реализация компонентов функции хеширования «Стрибог» ГОСТ Р 34.11-2012;

Программная реализация компонентов схемы электронной подписи ГОСТ Р 34.10-2012;

Построение криптографических протоколов с использованием ruToken CSP;

Контроль эффективности средств защиты, реализующих используемые криптографические протоколы и стандарты.

Рекомендуемый перечень основной литературы:

Аверченков В.И. Криптографические методы защиты информации [Текст] + [Электронный ресурс]: учебное пособие/ В.И. Аверченков, М.Ю. Рытов, С.А. Шпичак. – Брянск: БГТУ, 2011. – 216 с. – (Серия «Организация и технология защиты информации»)

Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. Основы криптографии. Учебное пособие / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. – М.: Гелиос-АРВ, 2001. – 480 с.

Алешников С.И. Математические методы защиты информации. Часть 3. Вычислительный практикум по числовым полям и криптографии в квадратичных полях [Электронный ресурс]: практическое пособие/ Алешников С.И., Козьминых Е.В.— Электрон. текстовые данные.— Калининград: Балтийский федеральный университет им. Иммануила Канта, 2006.— 97 c.— Режим доступа: http://www.iprbookshop.ru/23851.— ЭБС «IPRbooks», по паролю.

Алешников С.И. Математические методы защиты информации. Часть 4. Вычислительный практикум по эллиптическим кривым и криптографии на эллиптических кривых [Электронный ресурс]: практическое пособие/ Алешников С.И., Болтнев Ю.Ф.— Электрон. текстовые данные.— Калининград: Балтийский федеральный университет им. Иммануила Канта, 2007.— 58 c.— Режим доступа: http://www.iprbookshop.ru/23795.— ЭБС «IPRbooks», по паролю.

Перечень материально-технического обеспечения:

Специфического материально-технического обеспечения не требуется.

*Б.1.С.5.2 Дисциплина «Информационная безопасность открытых систем»*

Коды формируемых компетенций: *ОПК-5.2*

В результате изучения дисциплины студент должен

знать:

* методы и средства обеспечения информационной безопасности открытых информационных систем;;
* методы контроля, разработки эксплуатационной документации, обслуживания систем защиты информации открытых информационных систем;

уметь:

* применять методы и средства защиты информации открытых информационных систем;;
* разрабатывать эксплуатационную документацию, требования по эксплуатации систем защиты открытых информационных систем;

Примерное распределение часов: не менее 180 ч.

Форма контроля: *экзамен*

Содержание дисциплины:

Функциональная среда открытых систем. Интерфейсы прикладного программирования. Прикладная программа (приложение). Прикладная платформа. Программные средства промежуточного слоя. Архитектура и структура информационных систем. Структура открытой информационной системы. Архитектура открытых систем. Моделирование среды открытых систем. Референсная модель (OSI/ISO). Модель MUSIC. Модель MIC. Эталонная модель OSE/RM. Обобщенная модель среды открытых систем. Цели создания эталонной модели OSE/RM. Переносимость прикладного программного обеспечения и повторное его использование. Переносимость данных. Взаимодействие приложений. Взаимодействие с точки зрения административного управления и защиты информации.

Рекомендуемый перечень лабораторных работ:

Межсетевое экранирование в ОС Linux и трансляция сетевых адресов;

Межсайтовое выполнение сценариев XSS

Внедрение кода SQL;

Удалённое управление и туннелирование по протоколу SSH;

Система аутентификации, учёта и аудита в ОС Linux;

Стандартные сетевые утилиты. Сетевой сканер Nmap;

Анализатор трафика tcpdump;

Системы обнаружения вторжений;

Разработка эксплуатационной документацию по требования по эксплуатации систем защиты открытых информационных систем;

Контроль уровня защищенности VPN-сети.

Рекомендуемый перечень основной литературы:

Запечников С.В. Информационная безопасность открытых систем: Учебник для вузов. В двух томах. Том 1. Угрозы, уязвимости, атаки и подходы к защите / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков – М:. Горячая линия-Телеком, 2006. – 536.: ил.

Запечников С.В. Информационная безопасность открытых систем: Учебник для вузов. В двух томах. Том 2. Средства защиты в сетях / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков – М:. Горячая линия-Телеком, 2008. – 558.: ил.

Мельников Д.А. Информационная безопасность открытых систем : учебник / Д.А. Мельников. — М .: Ф ЛИНТА : Наука, 2013. — 448 с.

Шоу А. Логическое проектирование операционных систем = The Logical Design of Operating Systems. — М.: Мир, 1981. — 360 с.

Олифер В. Г., Олифер Н. А. Сетевые операционные системы. — СПб.: Питер, 2002. — 544 с. — ISBN 5-272-00120-6.

Перечень материально-технического обеспечения:

Специфического материально-технического обеспечения не требуется.

*Б.1.С.5.3 Дисциплина «Открытые информационные системы»*

Коды формируемых компетенций: *ОПК-5.3*

В результате изучения дисциплины студент должен

знать:

* основные информационные технологии, используемые в автоматизированных системах;
* системы управления информационной безопасностью открытой информационной системы;

уметь:

* работать с интегрированной средой разработки программного обеспечения;
* анализировать представленную в общедоступных источниках информацию о современных тенденциях в области информационных систем;

Примерное распределение часов: не менее 216 ч.

Форма контроля: *экзамен*

Содержание дисциплины:

Основные свойства и определения открытых систем. Модели и среды открытых информационных систем. Профили открытых информационных систем. Методология построения профилей информационных систем. Объекты стандартизации в функциональных профилях информационных систем. Компонентная разработка приложений.

Рекомендуемый перечень лабораторных работ:

Знакомство с виртуальными машинами и их классификация;

Знакомство с облачными хранилищами данных;

Основные функциональные возможности виртуальной машины Oracle VM Virtual Box;

Управление информационной безопасностью в виртуальной машине Oracle VM Virtual Box;

Запуск и настройка операционных систем в Oracle VM Virtual Box для обеспечения информационной безопасности.

Рекомендуемый перечень основной литературы:

Дубаков, А. А. Проектирование информационных и телекоммуникационных систем : учебное пособие [Электронный ресурс]/ А. А. Дубаков, А. Е. Пинжин ; Томский политехнический университет (ТПУ). — Томск : Изд-во ТПУ, 2014. — 424 с. : ил. .- Режим доступа http://www.iprbookshop.ru/46553– ЭБС «IPRbooks», по паролю.

Цилькер Б. Я., Орлов С.А. Организация ЭВМ и систем. [Электронный ресурс] СПб.: Питер, 2015. - 668 с. .- Режим доступа http://www.iprbookshop.ru/53410– ЭБС «IPRbooks», по паролю.

Эндрюс Г.Р. Основы многопоточного, параллельного и распределенного программирования.: Пер.с англ. - М.: Издательский дом ""Вильямс"", 2003. - 512 c.

Информационные системы и технологии в экономике : учеб.пособие / под ред. В. И. Лойко. - 2-е изд., перераб. и доп. - М. Финансы и статистика, 2005. - 413 с.

Гвоздева, Татьяна Вадимовна. Проектирование информационных систем: учебное пособие / Т. В. Гвоздева, Б. А. Баллод. — Ростов-на-Дону : Феникс, 2011. — 509 с. : ил.

Перечень материально-технического обеспечения:

Специфического материально-технического обеспечения не требуется.

*Б.1.С.6.1 Дисциплина «Платежные системы и их безопасность»*

Коды формируемых компетенций: *ОПК-6.1*

В результате изучения дисциплины студент должен

знать:

* подлежащие защите типовые технологические и бизнес-процессы организаций кредитно-финансовой сферы, в том числе связанные с осуществлением переводов денежных средств;
* основные угрозы безопасности информации при осуществлении переводов денежных средств с использованием платежных систем, пластиковых карт, систем дистанционного банковского обслуживания и др.;
* принципы формирования политики информационной безопасности в организациях кредитно-финансовой сферы

уметь:

* регистрировать события, связанные с защитой информации при реализации технологических и бизнес-процессов организаций кредитно-финансовой сферы, в том числе при осуществлении переводов денежных средств

Примерное распределение часов: не менее 144 ч.

Форма контроля: *зачет*

Содержание дисциплины:

Место и роль безналичных расчетов в рыночной экономике; теоретические основы формирования платежных и расчетных систем; формы и инструменты банковских расчетов; менеджмент информационной безопасности в платежных системах; зарубежные и международные платежные системы; система межбанковских расчетов в РФ; основы функционирования ведущих типов современных зарубежных платежных, расчетных систем и перспективы их развития; система «SWIFT»; банкоматы, POS-терминалы и пластиковые карты; дистанционное использование платежных систем; безопасность платежных систем.

Перечень материально-технического обеспечения:

Специфического материально-технического обеспечения не требуется.

*Б.1.С.6.2 Дисциплина «Нормативная база обеспечения информационной безопасности организаций финансово-кредитной сферы»*

Коды формируемых компетенций: *ОПК-6.3*

В результате изучения дисциплины студент должен

знать:

* стандарты в области обеспечения информационной безопасности организаций кредитно-финансовой сферы;
* требования к обеспечению информационной безопасности организаций кредитно-финансовой сферы;
* критерии оценки информационной безопасности организаций кредитно-финансовой сферы;
* требования к управлению риском нарушения информационной безопасности при аутсорсинге существенных функций

уметь:

* определять уровень обеспечения информационной безопасности организаций кредитно-финансовой сферы;
* оценивать риск нарушения информационной безопасности при аутсорсинге существенных функций

владеть:

* методикой оценки соответствия информационной безопасности организаций кредитно-финансовой сферы требованиям отраслевых стандартов

Примерное распределение часов: не менее 216 ч.

Форма контроля: *экзамен, зачет с оценкой*

Содержание дисциплины:

Банковская система РФ; платежные инструменты; автоматизированные банковские системы; риски ИБ; стандарты ИБ Банка России; аудит информационной безопасности в организациях кредитно-финансовой сферы; методика оценки соответствия информационной безопасности организаций банковской системы; информационная безопасность банков с учетом СТО БР ИББС; защита персональных данных в банках; политика ИБ, формирование СОИБ банковской организации.

Перечень материально-технического обеспечения:

Специфического материально-технического обеспечения не требуется.

*Б.1.С.6.3 Дисциплина «Управление инцидентами и непрерывностью бизнеса в организациях финансово-кредитной сферы»*

Коды формируемых компетенций: *ОПК-6.2*

В результате изучения дисциплины студент должен

знать:

* принципы выявления, учета и устранения инцидентов, возникающих в автоматизированных системах организаций кредитно-финансовой сферы;
* методы и способы обеспечения отказоустойчивости автоматизированных систем организаций кредитно-финансовой сферы

уметь:

* обнаруживать и устранять инциденты информационной безопасности, возникающие в процессе эксплуатации автоматизированных систем организаций кредитно-финансовой сферы

Примерное распределение часов: не менее 144 ч.

Форма контроля: *зачет*

Содержание дисциплины:

Международные и российские стандарты, регламентирующих управление инцидентами информационной безопасности и непрерывностью бизнеса; событие и инцидент информационной безопасности; цели и задачи управления информационной безопасностью; система управления инцидентами информационной безопасности; обнаружение событий информационной безопасности и инцидентов информационной безопасности и оповещение о них; реагирование на инциденты информационной безопасности; документация системы управления инцидентами информационной безопасности; группа реагирования на инциденты информационной безопасности; сохранение доказательств на инциденты информационной безопасности; средства управления событиями информационной безопасности; сбор и анализ технических данных при реагировании на инциденты информационной безопасности при осуществлении переводов денежных средств; определение непрерывности бизнеса и управление ей; система управления непрерывностью бизнеса; жизненный цикл управления непрерывностью бизнеса; документация и записи в области непрерывности бизнеса; готовность информационных и телекоммуникационных технологий к обеспечению непрерывности бизнеса; средства управления непрерывностью бизнеса.

Рекомендуемый перечень лабораторных работ:

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.

Развертывание IRP системы.

Передача инцидентов из SIEM системы. Получение фидов из сторонних источников.

Обработка инцидентов информационной безопасности. Отработка жизненного цикла инцидента информационной безопасности.

Перечень материально-технического обеспечения:

Специфического материально-технического обеспечения не требуется.

*Б.1.С.6.4 Дисциплина «Защита информации в автоматизированных системах организаций финансово-кредитной сферы»*

Коды формируемых компетенций: *ОПК-6.3*

В результате изучения дисциплины студент должен

знать:

* основные угрозы безопасности информации и модели нарушителя в автоматизированных системах организаций финансово-кредитной сферы;
* программно-аппаратные средства защиты информации автоматизированных систем организаций кредитно-финансовой сферы;
* криптографические средства и протоколы, используемые для защиты информации в автоматизированных системах организаций кредитно-финансовой сферы

уметь:

* определять подлежащие защите информационные ресурсы автоматизированных систем организаций кредитно-финансовой сферы;
* обеспечивать безопасность информации с учетом требований политики информационной безопасности в организациях кредитно-финансовой сферы;
* составлять комплекс правил, процедур и средств обеспечения информационной безопасности автоматизированных систем организаций кредитно-финансовой сферы;
* определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем в кредитно-финансовой сфере

Примерное распределение часов: не менее 180 ч.

Форма контроля: *экзамен*

Содержание дисциплины:

Классификация и характеристики автоматизированных банковских систем (АБС), эксплуатирующихся в ЦБ РФ и банковских организациях РФ; задачи ИБ в АБС; организация деятельности по обеспечению информационной безопасности в организациях кредитно-финансовой сферы; модели угроз и нарушителей; формирование и развитие системы расчетов Банка России, элементы платежной системы ЦБ РФ, технологии построения; характеристика структуры, оценка безопасности и надежности централизованной платежной системы РФ; сервисы срочных и не срочных платежей, другие платежные системы и сервисы Банка России, требования к кредитным организациям для осуществления деятельности в указанных системах; служба информационной безопасности коммерческого банка, функции и полномочия, организация деятельности; информационная безопасность неплатежных АБС, телекоммуникационных систем ЦБ РФ и организаций кредитно-финансовой сферы; контроль внедрения и эксплуатации СЗИ банковских информационных систем в соответствии со стандартами ИБ и защиты информации ЦБ РФ.

Перечень материально-технического обеспечения:

Специфического материально-технического обеспечения не требуется.

*Б.1.С.7.1 Дисциплина «Верификация безопасности информационных систем»*

Коды формируемых компетенций: *ОПК-7.2*

В результате изучения дисциплины студент должен

знать:

* основные меры по защите информации в автоматизированных системах ;
* принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем ;
* программно-аппаратные средства обеспечения защиты информации в программном обеспечении автоматизированных систем ;
* специфику конструктивного исполнения антенно-фидерных устройств ;
* основные тенденции развития теории и техники антенн и сверхвысокочастотных устройств;
* методы расчета и измерения основных параметров линий передачи сверхвысокочастотного диапазона

уметь:

* контролировать безотказное функционирование технических средств защиты информации;
* определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем ;
* проводить технико-экономическое обоснование проектных решений программно-аппаратных средств обеспечения защиты информации в автоматизированной системе с целью обеспечения требуемого уровня защищенности;
* производить измерение основных характеристик и параметров элементов антенно-фидерных устройств

владеть:

* методами выявления уязвимости информационно-технологических ресурсов автоматизированных систем ;
* методами расчета и измерения основных параметров устройств СВЧ, антенн и линий передачи сверхвысокочастотного диапазона

Примерное распределение часов: не менее 180 ч.

Форма контроля: *экзамен*

Содержание дисциплины:

Верификация ПО. Методы верификации ПО. Жизненный цикл ПО. Методы статического анализа ПО. Методы проверки моделей (model checking). Методы динамического анализа ПО. Варианты функционального тестирования.

Рекомендуемый перечень основной литературы:

1.Вельдер С.Э. , Лукин М.А. , Шалыто А.А. Яминов Б.Р. Верификация автоматных программ. Санкт-Петребург (СПб), ИТМО, 2011// http://e/lanbook/com/book/40774#autshors

2. Яхонтов С.В. Современные методы и инструменты формальных спецификаций и дедуктивной верификации императивных программ.: учебн. пособие, Санкт-Петребург, СПбГУ, 2014// <http://e/lanbook/com/book/94682#autshors>

Перечень материально-технического обеспечения:

Анализатор линейных коммуникаций УЛАН -2, Комплекс защиты Secret Net, нелинейный локатор SEL SP-61/M "Катран", Система виброакустической защиты "Соната-АВ", Система виброакустической защиты "Соната-РС-2".

*Б.1.С.7.2 Дисциплина «Анализ рисков информационной безопасности»*

Коды формируемых компетенций: *ОПК-7.3*

В результате изучения дисциплины студент должен

знать:

* национальные, межгосударственные и международные стандарты в области защиты информации;
* последствия от нарушения свойств безопасности информации;
* основные угрозы безопасности информации и модели нарушителя в автоматизированных системах

уметь:

* анализировать цели создания автоматизированных систем и задачи, решаемые автоматизированными системами;
* оценивать информационные риски в автоматизированных системах

Примерное распределение часов: не менее 216 ч.

Форма контроля: *экзамен*

Содержание дисциплины:

Основные понятия рискологии ИБ. Основные процессы и документация по управлению рисками. Ролевая структура организации, политика безопасности. Оценка риской информационной безопасности. Эксплуатация информационной системы и независимый аудит. Управление инцидентами информационной безопасности. Соответствие требованиям законодательства и модели угроз информационной безопасности.

Рекомендуемый перечень лабораторных работ:

1. Анализ модели угроз и уязвимостей

2. Разработка и управление политикой безопасности информационной системы

3. Документирование процессов внедрения разработок по оценке рисков

Рекомендуемый перечень основной литературы:

1. Семкин С.Н. Основы организационного обеспечения информационной безопасности объектов информатизации.: Учебное пособие.-М.: Гелиос АРВ, 2005.-185

2. Нестеров С.А. Основы информационной безопасности [Электронный ресурс]: учебное пособие - Спнкт-Петребург: Лань, 2017.- 324 с.

3. Галатенко В.А. Основы информационной безопасности [Электронный ресурс]: - Электрон. текстовые данные.- Интернет - Университет(ИНТУИТ), 2016, - 266 с.

Перечень материально-технического обеспечения:

БД угроз ФСТЭК <http://bdu.fstec.ru>

*Б.1.С.7.3 Дисциплина «Анализ безопасности информационных систем»*

Коды формируемых компетенций: *ОПК-7.1*

В результате изучения дисциплины студент должен

знать:

* технические средства контроля эффективности мер защиты информации;
* принципы организации и структуру систем защиты информации программного обеспечения автоматизированных систем;
* программно-аппаратные средства обеспечения защиты информации автоматизированных систем

уметь:

* выбирать меры защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы

владеть:

* навыками использования программно-аппаратных средств обеспечения безопасности информации в автоматизированных системах

Примерное распределение часов: не менее 216 ч.

Форма контроля: *экзамен*

Содержание дисциплины:

Политика безопасности. Сетевой аудит и место систем обнаружения вторжений. Классификация систем обнаружения вторжений. Интеллектуальное и поведенческое обнаружение вторжений.

Нормативная база управления инцидентами . Стандарт ISO 27035. Идентификация, протоколирование, реагирование на инциденты ИБ. Влияние инцидентов ИБ на бизнес-процессы. Организация и средства защиты информационных процес-сов в компьютерных системах. Средства управления событиями ИБ. SOC-центры ИБ, SIEM-системы управления информацией о безопасности и со-бытиями информационной безопасности, IRP-системы автоматизации реагирования на инциденты информационной без-опасности

Рекомендуемый перечень основной литературы:

1. Шелухин О.И. Обнаружение вторжений в компьютерные сети (сетевые аномалии). Учебное пособие [Электронный ресурс]: учебное пособие/ Шелухин О.И., САкалема Д.Ж., Филинова А.С.- электрон. дан.- Москва: Горячая линия-Телеком, 2013, - 220 с.

2. Милославская Н.Г. Интрасети: обнаружение вторжений: [учебн. пособие для студентов вузов по специальности информ. безоп. авт. систем и ""Компьютерная безопасность""]/ Н.Г. Миорславская , А.И. Толстой .- М.:ЮНИТИ-ДАНА, 2001 г.- 587 с.

3. В.Г. Миронова, А.А. Шелупанов. Анализ этапов предпроектного обследования информационной системы персональных данных // Периодический научный журнал «Вестник СибГАУ им.М.Ф.Решетнева».-2011 - №2(35), С. 45-48

4. А. Бирюков ""Информационная безопасность: защита и нападение"" 2-е изд. ДМК(2017)

Перечень материально-технического обеспечения:

Анализатор линейных коммуникаций УЛАН -2, Комплекс защиты информации "Secret ЮDisk" , Комплекс защиты "Secret Net", нелинейный локатор SEL SP-61/M "Катран", Система виброакустической защиты "Соната-АВ", Система виброакустической защиты "Соната-РС-2", средства ограничения доступа к компьютеру АПМДЗ "КРИПТОН-ЗАМОК/Е".

*Б.1.С.8.1 Дисциплина «Администрирование автоматизированных систем в защищенном исполнении»*

Коды формируемых компетенций: *ОПК-8.1*

В результате изучения дисциплины студент должен

знать:

* порядок установки и настройки сертифицированных операционных систем;
* порядок установки, настройки и обновления сертифицированного программного обеспечения и технических средств защиты информации;
* порядок проведения аудита защищенности автоматизированной системы

уметь:

* обосновывать целесообразность создания автоматизированной систем в защищенном исполнении;
* формировать исходные требования к автоматизированной систем в защищенном исполнении, процессу ее создания и эксплуатации

Примерное распределение часов: не менее 216 ч.

Форма контроля: *экзамен*

Содержание дисциплины:

Порядок установки и настройки сертифицированных операционных систем. Порядок установки, настройки и обновления программного обеспечения в соответствии с технической документацией. Управление пользователями и разграничение прав доступа к данным. Котроль целостноти подсистем защиты информации. Диагностика, устранение отказов и обеспечение работоспособности программно-аппаратных средств обеспечения информационной безопасности. Аудит защищенности автоматизированной системы. Установка и настройка технических средств защиты информации.

Рекомендуемый перечень лабораторных работ:

1. Установка и первичная настройка сертифицированной операционной системы

2. Управление пользователями и разграничение прав доступа к данным.

3. Аудит защищенности автоматизированной системы.

4. Установка и настройка технических средств защиты информации.

Рекомендуемый перечень основной литературы:

Буренин П.В., Девянин П.Н., Лебеденко Е.В. и др. Безопасность операционной системы специального назначения Astra Linux Special Edition Под ред. доктора техн. наук, профессора П.Н. Девянина. 3-е издание, перераб. и доп. Учебное пособие для вузов. М.: Горячая линия – Телеком, 2019. 404 с.: ил. ISBN 978-5-9912-0807-9.

Перечень материально-технического обеспечения:

Специфического материально-технического обеспечения не требуется.

*Б.1.С.8.2 Дисциплина «Организация проектной деятельности»*

Коды формируемых компетенций: *ОПК-8.2*

В результате изучения дисциплины студент должен

знать:

* базовые принципы и задачи проектной деятельности;
* содержание и этапы проектной десятельности по созданию автоматизированных систем в защищенном исполнении;
* методы и инструменты проведения исследований в ходе проектной деятельности

уметь:

* обеспечивать и осуществлять разработку проектных и организационных решений;
* анализировать и составлять нормативные методические документы по обеспечению информационной безопасности программно-аппаратными средствами

Примерное распределение часов: не менее 180 ч.

Форма контроля: *зачет*

Содержание дисциплины:

Базовые принципы и задачи проектной деятельности. Содержание и этапы проектной десятельности по созданию автоматизированных систем в защищенном исполнении. Методы и инструменты проведения исследований в ходе проектной деятельности. Представление результатов проектной деятельности. Документирование системы защиты информации автоматизированной системы в защищенном исполнении. Анализ и составление нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами, с учетом нормативных правовых актов.

Рекомендуемый перечень основной литературы:

1. Редько С.Г., Итс Т.А., Цветкова Н.А., Голубев С.А., Сурина А.В. Основы проектной деятельности: учебное пособие. Учебное пособие. Санкт петербург. 2018. 84 c. DOI: 10.18720/SPBPU/2/s18-134.

2. Михалкина, Е. В. Организация проектной деятельности : учебное пособие / Е. В. Михалкина, А. Ю. Никитаева, Н. А. Косолапова ; Южный фе- деральный университет. – Ростов-на-Дону : Издательство Южного федерального университета, 2016. – 146 с. ISBN 978-5-9275-1988-0.

Перечень материально-технического обеспечения:

Специфического материально-технического обеспечения не требуется.

*Б.1.С.8.3 Дисциплина «Информационная безопасность автоматизированных систем в защищенном исполнении»*

Коды формируемых компетенций: *ОПК-8.3*

В результате изучения дисциплины студент должен

знать:

* содержание и порядок выполнения работ на стадиях и этапах создания автоматизированных систем в защищенном исполнении;
* содержание и порядок выполнения работ по защите информации о создаваемой автоматизированной системе в защищенном исполнении;
* порядок установки, монтажа, настройки и технического обслуживания технических средств защиты информации в соответствии с требованиями эксплуатационной документации;
* порядок измерения параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа;
* порядок измерения параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации

уметь:

* проводить тестирование функций отдельных программных и программно-аппаратных средств защиты информации

Примерное распределение часов: не менее 216 ч.

Форма контроля: *экзамен*

Содержание дисциплины:

Содержание и порядок выполнения работ на стадиях и этапах создания автоматизированных систем в защищенном исполнении. Содержание и порядок выполнения работ по защите информации о создаваемой автоматизированной системе в защищенном исполнении. Защита информации техническими средствами. Порядок установки, монтажа, настройки и технического обслуживания технических средств защиты информации в соответствии с требованиями эксплуатационной документации. Порядок измерения параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа. Измерение параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации. Тестирование функций отдельных программных и программно-аппаратных средств защиты информации.

Перечень материально-технического обеспечения:

Специфического материально-технического обеспечения не требуется.

*Б.1.С.9.1 Дисциплина «Информационная безопасность автоматизированных систем на транспорте»*

Коды формируемых компетенций: *ОПК-9.1, ОПК-9.2, ОПК-9.3*

В результате изучения дисциплины студент должен

знать:

* особенности проектирования систем защиты информации автоматизированных систем на транспорте;
* особенности эксплуатации систем защиты информации автоматизированных систем на транспорте;
* основные угрозы и уязвимости, методы контроля защищенности автоматизированных систем на транспорте

уметь:

* проектировать систему защиты информации автоматизированных систем на транспорте;
* осуществлять внедрение систем защиты информации автоматизированных систем на транспорте;
* анализировать, прогнозировать и устранять угрозы информационной безопасности автоматизированных систем на транспорте в течение всего времени их применения

владеть:

* навыками применения методов и средств защиты информации при построении систем защиты информации автоматизированных систем на транспорте;
* навыками применения автоматизированных средств контроля защищенности автоматизированных систем на транспорте.

Примерное распределение часов: не менее 216 ч.

Форма контроля: *экзамен*

Содержание дисциплины:

Характеристика корпоративных автоматизированных систем на транспорте как объектов систем информационной безопасности. Методы и средства обеспечения информационной безопасности автоматизированных систем на транспорте.

Перечень материально-технического обеспечения:

Специфического материально-технического обеспечения не требуется.

*Б.1.С.9.2 Дисциплина «Информационная безопасность информационно-управляющих и информационно-логистических систем на транспорте»*

Коды формируемых компетенций: *ОПК-9.1, ОПК-9.2, ОПК-9.3*

В результате изучения дисциплины студент должен

знать:

* особенности проектирования систем защиты информации информационно-управляющих и информационно-логистических систем на транспорте;
* особенности эксплуатации систем защиты информации информационно-управляющих и информационно-логистических систем на транспорте;
* основные угрозы и уязвимости, методы контроля защищенности информационно-управляющих и информационно-логистических систем на транспорте

уметь:

* проектировать систему защиты информации информационно-управляющих и информационно-логистических систем на транспорте, в том числе автоматизированных систем управления технологическими процессами;
* осуществлять внедрение систем защиты информации информационно-управляющих и информационно-логистических систем на транспорте, в том числе автоматизированных систем управления технологическими процессами;
* анализировать, прогнозировать и устранять угрозы информационной безопасности информационно-управляющих и информационно-логистических систем на транспорте, в том числе автоматизированных систем управления технологическими процессами, в течение всего времени их применения

владеть:

* навыками применения методов и средств защиты информации при построении систем защиты информации информационно-управляющих и информационно-логистических систем на транспорте, в том числе автоматизированных систем управления технологическими процессами;
* навыками применения автоматизированных средств контроля защищенности информационно-управляющих и информационно-логистических систем на транспорте, в том числе автоматизированных систем управления технологическими процессами.

Примерное распределение часов: не менее 180 ч.

Форма контроля: *экзамен*

Содержание дисциплины:

Уязвимости автоматизированных систем управления технологическими процессами, информационно-управляющих и информационно-логистических систем на транспорте. Обеспечение информационной безопасности автоматизированных систем управления технологическими процессами, информационно-управляющих и информационно-логистических систем на транспорте.

Перечень материально-технического обеспечения:

Специфического материально-технического обеспечения не требуется.

*Б.1.С.9.3 Дисциплина «Анализ безопасности программного обеспечения автоматизированных систем на транспорте»*

Коды формируемых компетенций: *ОПК-9.1, ОПК-9.3*

В результате изучения дисциплины студент должен

знать:

* особенности анализа безопасности программного обеспечения при разработке систем защиты информации автоматизированных систем на транспорте;
* основные дефекты и уязвимости программного обеспечения автоматизированных систем на транспорте

уметь:

* проводить анализ безопасности программного обеспечения при разработке систем защиты информации автоматизированных систем на транспорте;
* выявлять дефекты и уязвимости в программном обеспечении автоматизированных систем на транспорте

владеть:

* навыками применения инструментальных средств анализа безопасности программного обеспечения при построении систем защиты информации автоматизированных систем на транспорте;
* навыками применения инструментальных средств анализа безопасности программного обеспечения автоматизированных систем на транспорте.

Примерное распределение часов: не менее 216 ч.

Форма контроля: *экзамен*

Содержание дисциплины:

Подтверждение соответствия информационно-управляющих и автоматизированных систем на транспорте. Сертификация средств защиты информации по требованиям безопасности информации. Методы и инструментальные средства анализа безопасности программного обеспечения информационно-управляющих и автоматизированных систем на транспорте.

Перечень материально-технического обеспечения:

Специфического материально-технического обеспечения не требуется.

*Б.1.С.9.4 Дисциплина «Технология защиты в корпоративных сетях передачи данных (по видам транспорта)»*

Коды формируемых компетенций: *ОПК-9.1, ОПК-9.2, ОПК-9.3*

В результате изучения дисциплины студент должен

знать:

* особенности проектирования систем защиты информации корпоративных сетей передачи данных (по видам транспорта);
* особенности эксплуатации систем защиты информации корпоративных сетей передачи данных (по видам транспорта);
* основные угрозы и уязвимости, методы контроля защищенности корпоративных сетей передачи данных (по видам транспорта)

уметь:

* проектировать систему защиты информации корпоративных сетей передачи данных (по видам транспорта);
* осуществлять внедрение систем защиты информации корпоративных сетей передачи данных (по видам транспорта);
* анализировать, прогнозировать и устранять угрозы информационной безопасности корпоративных сетей передачи данных (по видам транспорта)

владеть:

* навыками применения методов и средств защиты информации при построении систем защиты информации корпоративных сетей передачи данных (по видам транспорта);
* навыками применения инструментальных средств контроля защищенности корпоративных сетей передачи данных (по видам транспорта).

Примерное распределение часов: не менее 144 ч.

Форма контроля: *экзамен*

Содержание дисциплины:

Фильтрация сетевого трафика. Обеспечение качества обслуживания сетей передачи данных. Трансляция сетевых адресов. Групповое вещание. Протокол IPv6. Виртуальные частные сети.

Перечень материально-технического обеспечения:

Специфического материально-технического обеспечения не требуется.

*Б.1.С.10.1 Дисциплина «Планирование мероприятий по защите АСУ ТП»*

Коды формируемых компетенций: *ОПК-10.1*

В результате изучения дисциплины студент должен

знать:

* модель угроз информационной безопасности на предприятии (объекте) топливно-энергетического комплекса;
* локальные нормативные акты и другие документы, определяющие политику и правила обеспечения информационной безопасности на предприятии (объекте) топливно-энергетического комплекса

уметь:

* классифицировать и оценивать угрозы безопасности информации для значимых объектов критической информационной инфраструктуры на предприятии (объекте) топливно-энергетического комплекса;
* разрабатывать модели угроз безопасности информации и нарушителей в значимых объектах критической информационной инфраструктуры объектов топливно-энергетического комплекса;
* определять информационную инфраструктуру и информационные ресурсы значимых объектов критической информационной инфраструктуры объектов топливно-энергетического комплекса, подлежащие защите

Примерное распределение часов: не менее 216 ч.

Форма контроля: *экзамен*

Содержание дисциплины:

Модель угроз информационной безопасности на предприятии (по отрасли или в сфере профессиональной деятельности). Локальные нормативные акты и другие документы, определяющие политику и правила обеспечения информационной безопасности на предприятии (по отрасли или в сфере профессиональной деятельности). Методические и руководящие документы по защите информации в областях, относящихся к областям функционирования значимых объектов критической информационной инфраструктуры. Методические и руководящие документы по защите информации на значимых объектах критической информационной инфраструктуры. Методы организации и проведения технического обслуживания средств защиты информации.

Перечень материально-технического обеспечения:

Специфического материально-технического обеспечения не требуется.

*Б.1.С.10.2 Дисциплина «Проектирование, разработка и реализация систем защиты информации АСУ ТП»*

Коды формируемых компетенций: *ОПК-10.2*

В результате изучения дисциплины студент должен

знать:

* этапы проектирования систем защиты информации критически важных объектов;
* основные методические и руководящие документы по защите информации на значимых объектах критической информационной инфраструктуры;
* основную эксплуатационную и проектную документацию на информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, обеспечивающие функционирование топливно-энергетического комплекса

уметь:

* выбирать меры защиты информации, подлежащие реализации в системе защиты информации значимых объектов критической информационной инфраструктуры объектов топливно-энергетического комплекса;
* выбирать программно-аппаратные средства защиты информации для использования их в составе значимых объектов критической информационной инфраструктуры топливно-энергетического комплекса с целью обеспечения требуемого уровня защищенности информации;

владеть:

* навыками определения комплекса мер для защиты информации значимых объектов критической информационной инфраструктуры топливно-энергетического комплекса

Примерное распределение часов: не менее 216 ч.

Форма контроля: *экзамен*

Содержание дисциплины:

Этапы проектирования систем защиты информации критически важных объектов. Методические и руководящие документы по защите информации на значимых объектах критической информационной инфраструктуры. Эксплуатационная и проектная документация на информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, обеспечивающие функционирование предприятия (по отрасли или в сфере профессиональной деятельности). Криптографические методы, алгоритмы, протоколы, используемые для обеспечения защиты информации в значимых объектах критической информационной инфраструктуры объектов (по отрасли или в сфере профессиональной деятельности). Составные части АИСУ, жизненный цикл АСОИУ, виды проектов АСОИУ. Технические средства контроля эффективности мер защиты информации.

Рекомендуемый перечень лабораторных работ:

определение комплекса мер для защиты информации значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности);

обнаружение неисправностей в работе системы безопасности значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности);

устранение неисправностей в работе системы безопасности значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности);

Перечень материально-технического обеспечения:

Специфического материально-технического обеспечения не требуется.

*Б.1.С.10.3 Дисциплина «Аудит и оценка защищенности информационной безопасности АСУ ТП»*

Коды формируемых компетенций: *ОПК-10.3*

В результате изучения дисциплины студент должен

знать:

* технические средства контроля эффективности мер защиты информации;
* модель нарушителя информационной безопасности на предприятии (объекте) топливно-энергетического комплекса;
* основные системы и способы тестирования на проникновение;
* технические средства контроля эффективности мер защиты информации;
* модель нарушителя информационной безопасности на предприятии (объекте) топливно-энергетического комплекса;
* основные системы и способы тестирования на проникновение

уметь:

* определять источники и причины возникновения инцидентов;
* обнаруживать нарушения правил разграничения доступа;
* определять защищенность значимых объектов критической информационной инфраструктуры в соответствии с требованиями по безопасности;
* определять источники и причины возникновения инцидентов;
* обнаруживать нарушения правил разграничения доступа;
* определять защищенность значимых объектов критической информационной инфраструктуры в соответствии с требованиями по безопасности

Примерное распределение часов: не менее 180 ч.

Форма контроля: *зачет*

Содержание дисциплины:

Технические средства контроля эффективности мер защиты информации. Модель нарушителя информационной безопасности на предприятии (объекте) (по отрасли или в сфере профессиональной деятельности). Основные системы и способы тестирования на проникновение. Модель угроз информационной безопасности, модель нарушителя информационной безопасности на предприятии (объекте) (по отрасли или в сфере профессиональной деятельности). Методы анализа и оценки защищённости автоматизированных систем. Национальные и международные стандарты в области аудита и оценки информационной безопасности этапы и процедуры аудита информационной безопасности защищённых автоматизированных систем управления.

Перечень материально-технического обеспечения:

Специфического материально-технического обеспечения не требуется.

*Б.1.С.11.1 Дисциплина «Планирование мероприятий по защите ЗО КИИ»*

Коды формируемых компетенций: *ОПК-11.1*

В результате изучения дисциплины студент должен

знать:

* методику моделирования угроз информационной безопасности;
* локальные нормативные акты и другие документы, определяющие политику и правила обеспечения информационной безопасности на предприятии (объекте) топливно-энергетического комплекса

уметь:

* классифицировать и оценивать угрозы безопасности информации для значимых объектов критической информационной инфраструктуры на предприятии (объекте) топливно-энергетического комплекса;
* разрабатывать модели угроз безопасности информации и нарушителей в значимых объектах критической информационной инфраструктуры объектов топливно-энергетического комплекса;
* определять информационную инфраструктуру и информационные ресурсы значимых объектов критической информационной инфраструктуры объектов топливно-энергетического комплекса, подлежащие защите

Примерное распределение часов: не менее 216 ч.

Форма контроля: *экзамен*

Содержание дисциплины:

Модель угроз информационной безопасности на предприятии (по отрасли или в сфере профессиональной деятельности). Локальные нормативные акты и другие документы, определяющие политику и правила обеспечения информационной безопасности на предприятии (по отрасли или в сфере профессиональной деятельности). Методические и руководящие документы по защите информации в областях, относящихся к областям функционирования значимых объектов критической информационной инфраструктуры. Методические и руководящие документы по защите информации на значимых объектах критической информационной инфраструктуры. Методы организации и проведения технического обслуживания средств защиты информации.

Перечень материально-технического обеспечения:

MathCad

*Б.1.С.11.2 Дисциплина «Проектирование, разработка и реализация систем защиты ЗО КИИ»*

Коды формируемых компетенций: *ОПК-11.2*

В результате изучения дисциплины студент должен

знать:

* этапы проектирования систем защиты информации критически важных объектов; ;
* основные методические и руководящие документы по защите информации на значимых объектах критической информационной инфраструктуры;
* основную эксплуатационную и проектную документацию на информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, обеспечивающие функционирование топливно-энергетического комплекса

уметь:

* выбирать меры защиты информации, подлежащие реализации в системе защиты информации значимых объектов критической информационной инфраструктуры объектов топливно-энергетического комплекса;
* выбирать программно-аппаратные средства защиты информации для использования их в составе значимых объектов критической информационной инфраструктуры топливно-энергетического комплекса с целью обеспечения требуемого уровня защищенности информации;

владеть:

* навыками определения комплекса мер для защиты информации значимых объектов критической информационной инфраструктуры топливно-энергетического комплекса

Примерное распределение часов: не менее 216 ч.

Форма контроля: *экзамен*

Содержание дисциплины:

Этапы проектирования систем защиты информации критически важных объектов. Методические и руководящие документы по защите информации на значимых объектах критической информационной инфраструктуры. Эксплуатационная и проектная документация на информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, обеспечивающие функционирование предприятия (по отрасли или в сфере профессиональной деятельности). Криптографические методы, алгоритмы, протоколы, используемые для обеспечения защиты информации в значимых объектах критической информационной инфраструктуры объектов (по отрасли или в сфере профессиональной деятельности). Составные части АИСУ, жизненный цикл АСОИУ, виды проектов АСОИУ. Технические средства контроля эффективности мер защиты информации.

Рекомендуемый перечень лабораторных работ:

* определение комплекса мер для защиты информации значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности);
* обнаружение неисправностей в работе системы безопасности значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности);
* устранение неисправностей в работе системы безопасности значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности);

Перечень материально-технического обеспечения:

Специфического материально-технического обеспечения не требуется.

*Б.1.В.1 Дисциплина «Основы научных исследований»*

Коды формируемых компетенций: *ОПК-8*

В результате изучения дисциплины студент должен

знать:

* методологические основы научных исследований;
* порядок подготовки, выполнения и защиты квалификационных и иных научных работ (курсовые и дипломные работы, отчеты о НИР, диссертации и др.)

уметь:

* работать с научной, научно-технической и патентной литературой;
* обрабатывать результаты научных исследований

Примерное распределение часов: не менее 180 ч.

Форма контроля: *зачет*

Содержание дисциплины:

Методологические основы научного познания и творчества. Сущность знания и познания. Процесс научного исследования. Основные методы научных исследований. Элементы теории и методологии научно-технического творчества. Виды научных исследований. Обработка научной информации.

Перечень материально-технического обеспечения:

Специфического материально-технического обеспечения не требуется.

*Б.1.В.2 Дисциплина «Информатика»*

Коды формируемых компетенций: *ОПК-2*

В результате изучения дисциплины студент должен

знать:

* общие принципы построения современных компьютеров, формы и способы представления данных в персональном компьютере;
* логико-математические основы построения электронных цифровых устройств;
* состав, назначение аппаратных средств и программного обеспечения персонального компьютера

уметь:

* применять типовые программные средства сервисного назначения, информационного поиска и обмена данными в сети Интернет;
* составлять документы, используя прикладные программы офисного назначения;
* пользоваться средствами пользовательских интерфейсов операционных систем

Примерное распределение часов: не менее 108 ч.

Форма контроля: *зачет*

Содержание дисциплины:

Представление данных в компьютере. Основы устройства компьютера. Программное обеспечение компьютера. Компьютерные сети.

Рекомендуемый перечень лабораторных работ:

Представление числовых данных в памяти компьютера.

Представление нечисловых данных в памяти компьютера.

Моделирование функциональных блоков компьютера с помощью специальных программных средств.

Разработка документов сложной структуры с помощью программных средств офисного назначения.

Моделирование локальной сети с помощью программных средств виртуализации.

Перечень материально-технического обеспечения:

Специфического материально-технического обеспечения не требуется.

*Б.1.В.3 Дисциплина «Инженерная и компьютерная графика (Инженерная графика)»*

Коды формируемых компетенций: *ОПК-5*

В результате изучения дисциплины студент должен

знать:

* условные графические обозначения видов проводки, материалов конструкций, электронных компонентов в соответствии с требованиями ЕСПД и ЕСКД

уметь:

* использовать программные средства для построения графических схем и алгоритмов в соответствии с требованиями ЕСПД и ЕСКД

Примерное распределение часов: не менее 72 ч.

Форма контроля: *зачет*

Содержание дисциплины:

Методы проецирования. Прямая линия и плоскость. Кривые линии и поверхности. Аксонометрические проекции. Изображения предметов. Виды, разрезы, сечения. Основные требования ЕСКД к оформлению чертежей. Основные виды чертежей.

Рекомендуемый перечень лабораторных работ:

* Построение проекций линии пересечения двух пересекающихся многогранников.
* Построение проекций линии взаимного пересечения двух кривых поверхностей.
* Изображения по ЕСКД. Построение третьего вида модели по двум заданным.
* Построение сечений.
* Выполнение разрезов.
* Построение прямоугольной аксонометрической проекции

Перечень материально-технического обеспечения:

Специфического материально-технического обеспечения не требуется.

**Примерные программы практики**

Ознакомительная практика

Цель: расширение профессиональных знаний, полученных ими в процессе обучения и практических навыков ведения самостоятельной эксплуатационной и организационно-управленческой работы. Основной задачей практики является приобретение опыта практический деятельности и формирование профессиональных компетенций.

Формируемые компетенции: УК-2, УК-4, ОПК-8.

Эксплуатационная практика.

Цель: приобретение обучающимися опыта профессиональной деятельности, умений и навыков ведения самостоятельной научно-исследовательской, проектной, эксплуатационной организационно-управленческой работы.

Формируемые компетенции: УК-4, УК-6, ОПК-8.

Преддипломная практика

Преддипломная практика обеспечивает подготовку выпускной квалификационной работы, а также имеет целью закрепление профессиональных знаний и практических навыков ведения самостоятельной научно-исследовательской, проектной, эксплуатационной, контрольно-аналитической и организационно-управленческой работы, полученных обучающимися в процессе обучения.

Формируемые компетенции: УК-2, УК-4, УК-6, ОПК-8, ОПК-11.

**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; оригинальность и новизна полученных результатов.

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 требования к реализации программы специалитета

Организация должна располагать на праве собственности или ином законном основании материально-техническим обеспечением образовательной деятельности (помещениями и оборудованием) для реализации программы специалитета   
по Блоку 1 «Дисциплины (модули)» и Блоку 3 «Государственная итоговая аттестация» в соответствии с учебным планом.

Каждый обучающийся в течение всего периода обучения должен быть обеспечен индивидуальным неограниченным доступом к электронной информационно-образовательной среде Организации. 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.

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 РФ[[4]](#footnote-4).

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 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 в области:

- физики, оснащенную учебно-лабораторными стендами по механике, электричеству и магнетизму, 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;

- сетей и систем передачи информации, оснащенную рабочими местами на базе вычислительной техники, стендами сетей передачи информации с коммутацией пакетов и коммутацией каналов;

- безопасности компьютерных сетей, оснащенную стендами для изучения проводных и беспроводных компьютерных сетей, включающими абонентские устройства, коммутаторы, маршрутизаторы, средства анализа сетевого трафика, межсетевые экраны, средства обнаружения компьютерных атак, средства анализа защищенности компьютерных сетей;

- технической защиты информации, оснащенную специализированным оборудованием по защите информации от утечки по акустическому каналу и каналу побочных электромагнитных излучений и наводок, техническими средствами контроля эффективности защиты информации от утечки по указанным каналам;

- программно-аппаратных средств защиты информации, оснащенную антивирусными программными комплексами, аппаратными средствами аутентификации пользователя, средствами анализа программных реализаций, программно-аппаратными комплексами поиска и уничтожения остаточной информации, программно-аппаратными модулями доверенной загрузки, программно-аппаратными комплексами защиты информации, включающими в том числе средства криптографической защиты информации;

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.

Организация должна иметь лаборатории и (или) специально оборудованные кабинеты (классы, аудитории), обеспечивающие практическую подготовку в соответствии с каждой специализацией программы специалитета, которые она реализует.

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 обучаемого при проведении занятий в данных классах (лабораториях).

Допускается частичная замена оборудования его виртуальными аналогами.

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.

## 6.3. Требования к кадровым условиям 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).

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 2.3.6 «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».

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 специалитета, 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. Требования к финансовым условиям реализации программы специалитета

Финансовое обеспечение реализации программы специалитета должно осуществляться в пределах бюджетных ассигнований федерального бюджета, выделяемых федеральному органу исполнительной власти, в ведении которого находится образовательная организация.

## 6.5. Требования к применяемым механизмам 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 к0ачества образовательной деятельности по программе специалитета в рамках процедуры государственной аккредитации осуществляется с целью подтверждения соответствия образовательной деятельности по программе специалитета требованиям ФГОС ВО с учетом соответствующей ПООП.

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

10.05.03 «Информационная безопасность автоматизированных систем»

|  |  |  |
| --- | --- | --- |
| № п/п | Код профессионального стандарта | Наименование области профессиональной деятельности. Наименование профессионального стандарта |
| 06 Связь, информационные и коммуникационные технологии | | |
| 1. | 06.001 | Профессиональный стандарт «Программист», утвержденный приказом Министерства труда и социальной защиты Российской Федерации  от 18 ноября 2013 г. № 679н (зарегистрирован Министерством юстиции Российской Федерации 18 декабря 2013 г., регистрационный № 30635), 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) |
| 2. | 06.011 | Профессиональный стандарт «Администратор баз данных», утвержденный приказом Министерства труда и социальной защиты Российской Федерации  от 17 сентября 2014 г. № 647н (зарегистрирован Министерством юстиции Российской Федерации 24 ноября 2014 г., регистрационный № 34846), 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) |
| 3. | 06.026 | Профессиональный стандарт «Системный программист», утвержденный приказом Министерства труда и социальной защиты Российской Федерации  от 29 сентября 2020 г. № 678н (зарегистрирован Министерством юстиции Российской Федерации 26 октября 2020 г., регистрационный № 60582) |
| 4. | 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) |
| 5. | 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 22 ноября 2016 г., регистрационный № 44398) |
| 6. | 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) |
| 7. | 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) |
| 8. | 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 | | |
| 9. | 12.004 | Профессиональный стандарт, утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 29 декабря 2015 г. № 1179н (зарегистрирован Министерством юстиции Российской Федерации 28 января 2016 г., регистрационный № 40858) |
| 10. | 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 программ специалитета по направлению подготовки (специальности)

10.05.03 «Информационная безопасность автоматизированных систем»

| Код и наименование  профессионального  стандарта | Обобщенные трудовые функции | | | Трудовые функции | |
| --- | --- | --- | --- | --- | --- |
| Код | Наименование | Уровень квалиф. | Наименование | Код |
| 06.030 Специалист по защите информации в телекоммуникационных системах и сетях | A | Выполнение комплекса мер по обеспечению функционирования СССЭ (за исключением сетей связи специального назначения) и средств их защиты от НСД | 5 | Обеспечение бесперебойной работы СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем их защиты от НСД | A/02.5 |
| С | Обеспечение функционирования средств связи сетей связи специального назначения | 6 | Обеспечение бесперебойной работы средств связи сетей связи специального назначения, включая СКЗИ | С/02.6 |
| D | Разработка средств защиты СССЭ (за исключением сетей связи специального назначения) от НСД | 7 | Анализ угроз информационной безопасности в сетях электросвязи | D/01.7 |
| E | Обеспечение защиты средств связи сетей связи специального назначения от НСД | 7 | Организация функционирования сетей связи специального назначения и их средств связи | E/01.7 |
| 06.031 Специалист по автоматизации информационно-аналитической деятельности в сфере безопасности | D | Организационное управление в ИАС в защищенном исполнении | 7 | Управление работой коллектива информационно- аналитических работников и специалистов по созданию и эксплуатации ИАС | D/01.7 |
| A | Применение ИАС в защищенном исполнении в процессах АИАД | 7 | Решение типовых задач анализа  информации в ИАС государственных органов, обеспечивающих национальную безопасность | A/03.7 |
| Автоматизированная информационно-аналитическая поддержка процессов принятия решений | A/01.7 |
| E | Проведение исследований в области эффективных технологий АИАД | 8 | Анализ и обобщение результатов научных исследований и разработок в области технологий АИАД | E/01.8 |
| Моделирование и исследование технологий АИАД | E/02.8 |
| 06.032 Специалист по безопасности компьютерных систем и сетей | A | Обслуживание средств защиты информации в компьютерных системах и сетях | 5 | Обслуживание средств защиты информации прикладного и системного программного обеспечения | A/03.5 |
| B | Администрирование средств защиты информации в компьютерных системах и сетях | 6 | Администрирование подсистем защиты информации в операционных системах | B/01.6 |
| Администрирование программно-аппаратных средств защиты информации в компьютерных сетях | B/02.6 |
| Администрирование средств защиты информации прикладного и системного программного обеспечения | B/03.6 |
| С | Оценивание уровня безопасности компьютерных систем и сетей | 7 | Проведение анализа безопасности компьютерных систем | С/03.7 |
| Проведение инструментального мониторинга защищенности компьютерных систем и сетей | C/05.7 |
| 06.033 Специалист по защите информации в автоматизированных системах | A | Обслуживание систем защиты информации в автоматизированных системах | 5 | Проведение регламентных работ по эксплуатации систем защиты информации автоматизированных систем | А/01.5 |
| В | Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации | 6 | Управление защитой информации в автоматизированных системах | B/03.6 |
| С | Внедрение систем защиты информации автоматизированных систем | 6 | Разработка организационно-распорядительных документов по защите информации в автоматизированных системах | C/02.6 |
| Анализ уязвимостей внедряемой системы защиты информации | C/03.6 |
| D | Разработка систем защиты информации автоматизированных систем | 7 | Разработка программных и программно-аппаратных средств для систем защиты информации автоматизированных систем | D/04.7 |
| Разработка эксплуатационной документации на системы защиты информации автоматизированных систем | D/03.7 |
| Разработка проектных решений по защите информации в автоматизированных системах | D/02.7 |
| Тестирование систем защиты информации автоматизированных систем | D/01.7 |
| E | Формирование требований к защите информации в автоматизированных системах | 8 | Обоснование необходимости защиты информации в автоматизированной системе | E/01.8 |
| Моделирование защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации | E/04.8 |
| E | Определение угроз безопасности информации, обрабатываемой автоматизированной системой | 8 | Определение угроз безопасности информации, обрабатываемой автоматизированной системой | E/02.8 |
| 06.034 Специалист по технической защите информации | D | Проведение контроля защищенности информации | 6 | Проведение специальных исследований на побочные электромагнитные излучения и наводки технических средств обработки информации | D/01.6 |
| 6 | Проведение контроля защищенности информации от утечки за счет побочных электромагнитных излучений и наводок | D/02.6 |
| 6 | Проведение контроля защищенности акустической речевой информации от утечки по техническим каналам | D/03.6 |
| 6 | Проведение контроля защищенности информации от несанкционированного доступа | D/04.6 |
| F | Проектирование объектов в защищенном исполнении | 7 | Проектирование систем защиты информации на объектах информатизации | F/02.7 |
| I | Организация и проведение работ по технической защите информации | 8 | Создание системы защиты информации в организации | I/01.8 |
| 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 |
| 06.001 Программист | А | Разработка и отладка программного кода | 3 | Формализация и алгоритмизация поставленных задач | А/01.3 |
| Написание программного кода с использованием языков программирования, определения и манипулирования данными | А/02.3 |
| Оформление программного кода в соответствии с установленными требованиями | А/03.3 |
| Проверка и отладка программного кода | А/05.3 |
| В | Проверка работоспособности и рефакторинг кода программного обеспечения | 4 | Разработка тестовых наборов данных | В/02.4 |
| D | Разработка требований и проектирование программного обеспечения | 6 | Проектирование программного обеспечения | D/03.6 |
| 06.011 Администратор баз данных | А | Обеспечение функционирования БД | 4 | Управление доступом к БД | А/03.4 |
| Установка и настройка ПО для администрирования БД | А/05.4 |
| В | Оптимизация функционирования БД | 5 | Оптимизация выполнения запросов к БД | В/05.5 |
| Оптимизация управления жизненным циклом данных, хранящихся в БД | В/06.5 |
| С | Предотвращение потерь и повреждений данных | 5 | Выполнение процедур по вводу в рабочий режим ресурсов горячей замены | С/15.5 |
| D | Обеспечение информационной безопасности на уровне БД | 6 | Подготовка отчетов о состоянии и эффективности системы безопасности на уровне БД | D/05.6 |
|  | E | Управление развитием БД | 7 | Анализ системных проблем обработки информации на уровне БД, подготовка предложений по перспективному развитию БД | E/01.7 |

Приложение 3

Примерный календарный учебный график   
программы специалитета по направлению подготовки 10.05.03   
«Информационная безопасность автоматизированных 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 | ээ | кк | кк |  |  | п |  | п |  | п |  | п |  | п |  | п |  |  | 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 | кк | кк |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | ээ | ээ | ээ | ээ | кк | кк | кк | кк | кк | кк | кк | кк | кк | кк |
| **4 курс** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | ээ | ээ | ээ | кк | кк |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | ээ | ээ | ээ | ээ | кк | кк | кк | кк | кк | кк | кк | кк | кк | кк |
| **5 курс** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | ээ | ээ | ээ | кк | кк | пп | пп |  |  |  |  |  |  |  |  |  |  |  |  |  | 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 | пп | пп | пп | пп | пп | пп | пп | пп | гг | гг | гг | гг | кк |  | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Обозначения:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  | э |  |  |  |  | г |  |  |  |  | п |  |  |  |  | к |  |  |
| теоретическое обучение | | | | | экзаменационные сессии | | | | | государственная итоговая 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)
4. Федеральный [закон](consultantplus://offline/ref=6C7ED189C16CD34C808DC92023D3512929E2ACCF374AE36CABB52EE859N7r8K) от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3448; 2019, № 12, ст. 1221), Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3451; 2018, № 1, ст. 82). [↑](#footnote-ref-4)