**МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ,
СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»
(СПбГУТ)**

---

УТВЕРЖДАЮ
Декан ИКСС

Д.В. Окунева

# СБОРНИК АННОТАЦИЙ

рабочих программ дисциплин

образовательной программы высшего образования

Специальность «10.05.02 Информационная безопасность телекоммуникационных систем»,

специализация

«специализация N 9 "Управление безопасностью телекоммуникационных систем и сетей"»

Санкт-Петербург

## 1. Аннотации рабочих программ дисциплин (модулей) базовой части

### *Б1.О.01 История (история России, всеобщая история)*

Цели освоения дисциплины

Целью преподавания дисциплины «История (история России, всеобщая история)» является:

1) формирование систематизированных знаний об основных закономерностях и особенностях исторического процесса; 2) определение места россиискоЙ цивилизации в мировом историческом процессе с учетом стремления к объективности в его освещении; 3)раскрытие специфики историческои роли и ценностеи россиискои цивилизации; 4) формирование гражданской позиции и воспитание патриотизма; 5) формирование критического мышления и аналитических способностей.

Место дисциплины в структуре ОП

Дисциплина «История (история России, всеобщая история)» Б1.О.01 является дисциплиной обязательной части учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Изучение дисциплины «История (история России, всеобщая история)» основывается на базе знаний, умений и компетенций, полученных студентами в ходе освоения школьных курсов.

Требования к результатам освоения

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма (ОПК-17)
– Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия (УК-5)

Содержание дисциплины

Раздел 1. Введение в историческую науку
История как наука: предмет, цели, задачи изучения. Сущность, формы и функции исторического знания. Исторический источник: понятие и классификация. Виды источников.
Раздел 2. Методология исторической науки
Методология истории. Историография истории. История России как неотъемлемая часть

всемирной истории. Вспомогательные исторические дисциплины.
Раздел 3. Русские земли и мир в Средние века (V – XV вв.)
Восточное славянство в VII – сер. IX вв. Русь в IX - нач. XI вв. Научные дискуссии о понятии "российская цивилизации". Восточные славяне: расселение, быт, верования, хозяйственные занятия, родоплеменные отношения. Взаимоотношения восточных славян с соседями.Формирование территории Древней Руси. Отношения восточнославянских племен с соседними народами. Формирование древнерусского государства. Институт княжеской власти и его развитие в IX – XI вв. Города и их роль в системе административных и политических отношений Древней Руси. Древнерусское право. Категории свободного и зависимого населения. Экономическое развитие Древней Руси. Роль международной торговли по пути «Из варяг в греки». Развитие частного землевладения: особенности княжеской и боярской вотчин. Крещение Руси. Картина мира древнерусского человека. Внешняя политика киевских князей. Связи Руси с европейскими странами и народами. Древняя Русь и Византия. Дипломатия Древней Руси. Культура Древней Руси. Повседневная жизнь и быт. Восточное славянство в VII – сер. IX вв. Русь в IX - нач. XI вв. Научные дискуссии о понятии "российская цивилизации". Восточные славяне: расселение, быт, верования, хозяйственные занятия, родоплеменные отношения. Взаимоотношения восточных славян с соседями.Формирование территории Древней Руси. Отношения восточнославянских племен с соседними народами. Формирование древнерусского государства. Институт княжеской власти и его развитие в IX – XI вв. Города и их роль в системе административных и политических отношений Древней Руси. Древнерусское право. Категории свободного и зависимого населения. Экономическое развитие Древней Руси. Роль международной торговли по пути «Из варяг в греки». Развитие частного землевладения: особенности княжеской и боярской вотчин. Крещение Руси. Картина мира древнерусского человека. Внешняя политика киевских князей. Связи Руси с европейскими странами и народами. Древняя Русь и Византия. Дипломатия Древней Руси. Культура Древней Руси. Повседневная жизнь и быт.
Раздел 4. Россия и мир в XVI – XVII вв.
Развитие процесса централизации России в XVI в. Судебник 1550 г. Сложности и противоречия в развитии российской государственности. Развитие крепостнических тенденций. Борьба за присоединение к России западнорусских и южнорусских земель. Присоединение Великой Перми, колонизация Поволжья, Приуралья. Начало присоединения Зап. Сибири. Культура России втор. пол. XV-XVI вв. Смутное время. Ведущие мировые исторические события указанного периода
Раздел 5. Россия и мир в XVIII в.
Эпоха Петра I. Эпоха Дворцовых переворотов. Правление Екатерины Великой: просвещенный абсолютизм. Россия в системе международных отношений XVIII вв.
Раздел 6. Россия и мир в XIX в.
Участие в антинаполеоновских коалициях. Отечественная война 1812 г. "Священный союз". Россия в центре европейский дипломатии. Неосуществленные замыслы реформ и разочарование общества. Ориентация на использование принципов авторитаризма. Сверхцентрализация госуправления. Включение дворянского самоуправления в систему госвласти. Идеология самодержавия. Теория официальной народности. Политика в области просвещения и образования. Попытки решения назревших социально-экономических и политических проблем традиционными методами. Европейские революции 1848-49 гг. Состояние восточного вопроса. Причины, этапы и ход Крымской войны. Российская культура в пер. пол. XIX в. Внутреннее и международное положение России в сер. XIX в. Содержание и характер крестьянской реформы. Сельское хозяйство после реформы 1861 г. Новый этап в гражданском "раскрепощении". Новое земское и

городское положения. Политика в области просвещения и цензуры. Общественное движение в 80 - нач. 90-х гг. XIX в. Внешняя политика России в пореформенный период. Восточный вопрос. А. Горчаков. Россия и объединение Германии. Борьба за пересмотр условий Парижского мирного договора. "Союз трех императоров". Отношения России с Китаем, Японией и США. Присоединение к России Средней Азии. Оформление франко-русского союза. Русская культура XIX в.
Раздел 7. Россия и мир в XX вв.
Причины и последствия событий 25 октября 1917 г. Гражданская война и интервенция, их результаты и последствия. Российская эмиграция. Социально-экономическое развитие страны в 20-е гг. НЭП. Формирование однопартийного политического режима. Образование СССР. Культурная жизнь страны в 20-е гг. Внешняя политика. Курс на строительство социализма в одной стране и его последствия. Социально-экономические преобразования в 30-е гг. СССР накануне и в начальный период второй мировой войны. Великая Отечественная война. Социально-экономическое развитие, общественно-политическая жизнь, культура, внешняя политика СССР в послевоенные годы. Холодная война. Попытки осуществления политических и экономических реформ. СССР в середине 60-80-х гг.: нарастание кризисных явлений. Советский Союз в 1985-1991 гг. Постсоветский период в истории России. Перестройка. Распад СССР. Октябрьские события 1993 г. Становление новой российской государственности (1993-99 гг.).
Раздел 8. Россия и мир в начале XXI вв.
Россия на пути радикальной социально-экономической модернизации. Культура в современной России. Внешнеполитическая деятельность в условиях новой геополитической ситуации.
Раздел 9. Мировая история в начале XXI вв.
Ключевые мировые события в оценке современной исторической школы
Раздел 10. Новейшая история России
Ключевые отечественные события в оценке современной исторической школы

---

Общая трудоемкость дисциплины

144 час(ов), 4 ЗЕТ

Форма промежуточной аттестации

Экзамен

### *Б1.О.02 Физическая культура и спорт*

Цели освоения дисциплины

---

Целью преподавания дисциплины «Физическая культура и спорт» является: изучение и формирование физической культуры личности и способности направленного использования разнообразных средств физической культуры, спорта и туризма для сохранения и укрепления здоровья, психофизической подготовки и самоподготовки к будущей жизни и профессиональной деятельности

---

Место дисциплины в структуре ОП

Дисциплина «Физическая культура и спорт» Б1.О.02 является дисциплиной обязательной части учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Изучение дисциплины «Физическая культура и спорт» основывается на базе знаний, умений и компетенций, полученных студентами в ходе освоения школьных курсов.

Требования к результатам освоения

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности (УК-7)

Содержание дисциплины

Раздел 1. Теоретические основы физической культуры.
Физическая культура в профессиональной подготовке студентов и социокультурное развитие личности студента. Социально-биологические основы физической культуры. Основы здорового образа жизни и его отражение в профессиональной деятельности. Общая физическая и спортивная подготовка студентов в системе физического воспитания. Методические основы самостоятельных занятий физическими упражнениями и самоконтроль в процессе занятий. Профессионально-прикладная физическая подготовка будущих специалистов
Раздел 2. Базовый комплекс упражнений по общей физической подготовке.
Комплексы упражнений общей физической подготовки тренировочной направленности: общее оздоровление организма; поддержание спортивной формы на определенном уровне; комплексное развитие физических качеств; комплексная проработка мышечных групп
Раздел 3. Основные разделы физической подготовки.
Физические упражнения из разделов: гимнастика и атлетическая подготовка, ускоренное передвижение и легкая атлетика, спортивные и подвижные игры

Общая трудоемкость дисциплины

72 час(ов), 2 ЗЕТ

Форма промежуточной аттестации

Зачет

***Б1.О.03 Иностранный язык***

Цели освоения дисциплины

Целью преподавания дисциплины «Иностранный язык» является:
Целью преподавания дисциплины «Иностранный язык» является: повышение исходного уровня владения иностранным языком, достигнутого на предыдущей ступени образования, и овладение студентами необходимым и достаточным уровнем коммуникативной компетенции для решения социально-коммуникативных задач в различных областях бытовой, культурной, профессиональной и научной деятельности при общении с зарубежными партнерами, а также для дальнейшего самообразования

Место дисциплины в структуре ОП

Дисциплина «Иностранный язык» Б1.Б.03 является базовой дисциплиной цикла учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Изучение дисциплины «Иностранный язык» основывается на базе знаний, умений и компетенций, полученных студентами в ходе освоения школьных курсов.

Требования к результатам освоения

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия (УК-4)
– Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия (УК-5)

Содержание дисциплины

Раздел 1. Социально-культурная сфера общения
Социализация в мультикультурном пространстве. Основы межкультурной и деловой коммуникации. Вопросы образования в России и за рубежом. Совершенствование лексико-грамматических и фонетических навыков. Развитие продуктивных (говорение, письмо) и рецептивных (аудирование, чтение) видов речевой деятельности
Раздел 2. Учебно-познавательная сфера общения
Наука и техника. Научные открытия и персоналии, определившие направления развития связи и телекоммуникаций. Карьера в ИКТ. Совершенствование лексико-грамматических и фонетических навыков. Развитие продуктивных (говорение, письмо) и рецептивных (аудирование, чтение) видов речевой деятельности
Раздел 3. Профессиональная сфера общения. Современные ИКТ: общие проблемы

Инфокоммуникационные технологии. Разнообразие вычислительной техники. Компоненты компьютерной системы.. Совершенствование лексико-грамматических и фонетических навыков. Развитие продуктивных (говорение, письмо) и рецептивных (аудирование, чтение) видов речевой деятельности
Раздел 4. Профессиональная сфера общения (продолжение). Деловое общение
Научно-технический прогресс и его достижения в сфере инфокоммуникационных технологий и систем связи. Плюсы и минусы всеобщей информатизации. Совершенствование лексико-грамматических и фонетических навыков. Развитие продуктивных (говорение, письмо) и рецептивных (аудирование, чтение) видов речевой деятельности

---

Общая трудоемкость дисциплины

360 час(ов), 10 ЗЕТ

Форма промежуточной аттестации

Экзамен

***Б1.О.04 Экономика***

Цели освоения дисциплины

---

Целью преподавания дисциплины «Экономика» является:
умение анализировать информацию, необходимую для принятия обоснованных экономических решений и прогнозирования их последствий, применение полученных знаний в сфере личного экономического и финансового планирования; применение нормативных правовых актов при принятии экономических решений.

---

Место дисциплины в структуре ОП

---

Дисциплина «Экономика» Б1.О.04 является одной из дисциплин обязательной части учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Философия».

---

Требования к результатам освоения

---

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен принимать обоснованные экономические решения в различных областях жизнедеятельности (УК-10)

---

Содержание дисциплины

---

Раздел 1. Место, роль и функции государства в экономике.
Краткий обзор этапов развития экономической мысли. Предмет и метод экономической мысли. Предмет и метод экономической теории. Базовые экономические понятия. Экономические системы. Институциональные основы функционирования рынка.
Раздел 2. Спрос, предложение и рыночное равновесие
Спрос и его факторы. Предложение и его факторы. Рыночное равновесие и его устойчивость. Государственное регулирование индивидуальных рынков.
Раздел 3. Эластичность спроса и предложения, доходы
Эластичность спроса по цене. Факторы ценовой эластичности спроса. Взаимосвязь ценовой эластичности спроса и общей выручки продавцов. Эластичность спроса по доходу. Перекрестная эластичность спроса. Эластичность предложения. Основные виды доходов. Финансовые инструменты. Виды и источники возникновения экономических и финансовых рисков в экономике.
Раздел 4. Издержки производства. Фирма в условиях совершенной конкуренции
Фирма. Экономические и бухгалтерские издержки фирмы. Постоянные, переменные, общие, средние и предельные издержки фирмы. Издержки в длительном периоде. Совершенная и несовершенная конкуренция. Правило максимизации прибыли фирмы. Точка безубыточности, точка закрытия и кривая предложения конкурентной фирмы.
Раздел 5. Фирма в условиях несовершенной конкуренции
Монополия. Максимизация прибыли монополий. Ценовая дискриминация. Ущерб, наносимый монополией обществу. Государственная антимонопольная политика. Олигополия. Модели олигополии: ценовая война, ломаная кривая спроса, картель, лидерство в ценах. Монополистическая конкуренция. Равновесие фирмы на рынке монополистической конкуренции в краткосрочном и долгосрочном периодах.
Раздел 6. Основные макроэкономические показатели. Модель общего экономического равновесия
Валовый внутренний продукт (ВВП) и принципы его расчета. Валовый национальный продукт, чистый национальный продукт, национальный доход, личный доход, личный располагаемый доход. Дефлятор ВВП и Индекс потребительских цен. Макроэкономическая производственная функция. Функция потребления, инвестиционная функция. Роль ставки ссудного процента в установлении равновесия. Равновесие на финансовых рынках. Эффект вытеснения.
Раздел 7. Макроэкономическая нестабильность: инфляция и безработица
Сущность, функции и виды денег. Количественная теория денег и основная причина инфляции. Сеньораж. Гиперинфляция и пути её подавления. Общественные издержки инфляции. Измерение уровня безработицы. Основные причины безработицы. Закон Оукена. Кривая Филлипса.
Раздел 8. Теория экономических колебаний. Модель совокупного спроса и совокупного предложения (AD-AS)
Краткосрочные и долгосрочные экономические колебания. Кривая совокупного спроса AD и её сдвиги. Краткосрочная и долгосрочная кривые совокупного предложения. Равновесие в краткосрочном и долгосрочном периодах.
Раздел 9. Влияние кредитно- денежной политики на совокупный спрос. Кейнсианская теория национального дохода.

Шоки со стороны совокупного спроса и совокупного предложения. Политика стабилизации. Модель кейнсианского креста. Парадокс бережливости. Модель кейнсианского креста. Парадокс бережливости.
Раздел 10. Цели, задачи и инструменты бюджетно-налоговой, денежно-кредитной политики государства.
Мультипликатор государственных расходов, налоговый мультипликатор. Нормативные правовые акты, регламентирующие вопросы реализации бюджетно-налоговой и денежно-кредитной политики. Требования антикоррупционного законодательства.

---

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

***Б1.О.05 Философия***

Цели освоения дисциплины

---

Целью преподавания дисциплины «Философия» является:
формирование философской культуры мышления, осознанного отношения к наиболее общим принципам познания и практической деятельности, способности критического анализа и совместного обсуждения идей универсального характера.

---

Место дисциплины в структуре ОП

---

Дисциплина «Философия» Б1.О.05 является одной из дисциплин обязательной части учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «История».

---

Требования к результатам освоения

---

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий (УК-1)

---

Содержание дисциплины

Раздел 1. Введение в философию
Что такое философия? Особенности философского мышления. Отличия от др. форм знания и наук. Связь с другими сферами интеллектуальной деятельности. Основные понятия философии.
Раздел 2. Структура философии как предмета изучения. Часть 1: метафизика
Особенности структуры философии. Философские теоретические науки: метафизика, онтология, гносеология (эпистемология), формальная и диалектическая логики.
Раздел 3. Структура философии как предмета изучения. Часть 2: философская антропология.
Философские практические науки: этика, эстетика, аксиология, философская антропология и социальная философия и др. науки гуманитарного цикла, в которых применяется философский подход к решению насущных проблем.
Раздел 4. История философии. Часть 1: Античность и философия эпохи эллинизма.
Философские учения досократиков (Милетская школа философии о природе сущего). Элейская школа философии о едином бытии и учение Гераклита о становлении. Пифагорейство и античный атомизм. Софистика и Сократ (Горгий, Протагор). Философское учение Платона об идеях, познании, о добродетелях и государстве. Основные понятия метафизики Аристотеля. Физика, этика, политика и логические труды Аристотеля. Философия эпохи эллинизма. Общие черты эллинистической философии. Основные понятия кинизма, эпикуреизма, стоицизма, скептицизма.
Раздел 5. История философии. Часть 2: Античное начало и Средние века, философия эпохи Возрождения.
Библейская традиция и христианское богословие. Бог-творец и понятие креации. Время и мировая история. Христианская антропология и мистика, ее рецепция в исламе. Вопрос о соотношении веры и знания в схоластике. Спор об универсалиях (реализм, номинализм, концептуализм). Гуманистический пафос философии Возрождения.
Раздел 6. История философии. Часть 3: Новое время. Философия эпохи Просвещения.
Обоснование экспериментального метода Ф. Бэконом. Эмпиризм Т. Гоббса и Дж. Локка. Рациональная метафизика Р. Декарта, Б. Спинозы, Г. Лейбница. Антиклерикальный и антимонархический пафос философии Просвещения. Просветительские идеи в Англии, Франции, Германии, России.
Раздел 7. История философии. Часть 4: И. Кант и немецкая классическая философия.
Трансцендентальная философия И.Канта: новый взгляд на физику, мораль, искусство. Общий замысел и основные понятия наукоучения И. Фихте. Философия тождества Ф. Шеллинга. Диалектический метод в систематической философии Г. Гегеля.
Раздел 8. История философии. Часть 5: Марксизм и позитивизм, постклассическая философия.
Позитивизм: этапы развития. Рецепция диалектики Гегеля в марксизме. Иррационалистические настроения в философии XIX-XX веков.
Раздел 9. История философии. Часть 6: Русская философия.
Историософия П.Я. Чаадаева. Спор славянофилов и западников. Философия всеединства В.С. Соловьева. Религиозно-философские искания начала XX века. Марксизм в России. Представители неотомизма и неопатристический синтез русского зарубежья XX века.
Раздел 10. История философии. Часть 7: основные тенденции второй половины XX века.
Основные понятия феноменологической философии. Философская герменевтика. Онтологический стиль мышления М. Хайдеггера. Современный кризис естественных наук и его философская оценка.

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

***Б1.О.06 Безопасность жизнедеятельности***

Цели освоения дисциплины

Целью преподавания дисциплины «Безопасность жизнедеятельности» является:

формирование профессиональной культуры безопасности, предполагающей готовность и способность выпускника использовать приобретенную совокупность знаний, умений и навыков для обеспечения безопасности в сфере профессиональной деятельности и в условиях чрезвычайных ситуаций и военных конфликтов; формирование нетерпимого отношения к проявлениям экстремизма, терроризма и противодействия им в профессиональной и повседневной деятельности; получение знаний, умений и навыков, необходимых для становления обучающихся вузов в качестве граждан способных и готовых к выполнению воинского долга и обязанности по защите своей Родины в соответствии с законодательством РФ

Место дисциплины в структуре ОП

Дисциплина «Безопасность жизнедеятельности» Б1.О.06 является дисциплиной обязательной части учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Изучение дисциплины «Безопасность жизнедеятельности» основывается на базе знаний, умений и компетенций, полученных студентами в ходе освоения школьных курсов.

Требования к результатам освоения

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– 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-8)

– Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности (УК-11)

---

Содержание дисциплины

---

Раздел 1. Общевоинские уставы ВС РФ
Общевоинские уставы Вооруженных Сил Российской Федерации, их основные требования и содержание. Внутренний порядок и суточный наряд. Общие положения Устава гарнизонной и караульной службы
Раздел 2. Строевая подготовка
Строевые приемы и движение без оружия
Раздел 3. Огневая подготовка из стрелкового оружия
Основы, приемы и правила стрельбы из стрелкового оружия. Назначение, боевые свойства, материальная часть и применение стрелкового оружия, ручных противотанковых гранатометов и ручных гранат. Выполнение упражнений учебных стрельб из стрелкового оружия
Раздел 4. Основы тактики общевойсковых подразделений
Вооруженные Силы Российской Федерации их состав и задачи. Тактико-технические характеристики основных образцов вооружения и техники ВС РФ. Основы общевойскового боя. Основы инженерного обеспечения. Организация воинских частей и подразделений, вооружение, боевая техника вероятного противника
Раздел 5. Радиационная, химическая и биологическая защита
Ядерное, химическое, биологическое, зажигательное оружие. Радиационная, химическая и биологическая защита
Раздел 6. Военная топография
Местность как элемент боевой обстановки. Измерения и ориентирование на местности без карты, движение по азимутам. Топографические карты и их чтение, подготовка к работе. Определение координат объектов и целеуказания по карте
Раздел 7. Основы медицинского обеспечения
Медицинское обеспечение войск (сил), первая медицинская помощь при ранениях, травмах и особых случаях
Раздел 8. Военно-политическая подготовка
Россия в современном мире. Основные направления социально-экономического, политического и военно-технического развития страны
Раздел 9. Правовая подготовка
Военная доктрина РФ. Законодательство Российской Федерации о прохождении военной службы
Раздел 10. Опасности в сфере профессиональной деятельности, при угрозе возникновения чрезвычайных ситуаций и военных конфликтов
Физические негативные факторы и защита от их воздействия: вибрация, шум, инфразвук, ультразвук, электромагнитные излучения, тепловые излучения, лазерное излучение, ультрафиолетовые излучения, ионизирующие излучения, электрический ток и статическое электричество, механические факторы и факторы комплексного характера. Биологические негативные факторы; химические негативные факторы (вредные вещества). Опасные факторы при угрозе возникновения чрезвычайных ситуаций и военных конфликтов
Раздел 11. Методы оценки опасностей в сфере профессиональной деятельности и прогнозирование последствий в чрезвычайных ситуациях

Инструментальный контроль основных параметров производственной среды: микроклимат, уровень аэроионного состава воздуха, освещенность, зашумлённость. Исследование опасностей трехфазных сетей переменного тока. Прогнозирование последствий аварий на взрывоопасных, химических и радиационных промышленных объектах. Первая помощь при остановке сердца (базовая реанимация)
Раздел 12. Безопасные условия жизнедеятельности для сохранения природной среды и обеспечения устойчивого развития общества
Законодательство РФ о защите окружающей среды, промышленной безопасности, пожарной безопасности и чрезвычайных ситуациях. Экологическая безопасность в повседневной жизни и в профессиональной деятельности для сохранения природной среды и обеспечения устойчивого развития общества
Раздел 13. Правовые нормы противодействия экстремизму, терроризму и алгоритмы действий при террористической угрозе
Сущность проявления экстремизма и терроризма. Терроризм в XXI веке. Основные факторы, обусловливающие возникновение терроризма в Российской Федерации. Система противодействия терроризму в Российской Федерации. Рекомендации гражданам от Национального антитеррористического комитета и ФСБ России при террористической угрозе. Алгоритмы действий при террористической угрозе

---

Общая трудоемкость дисциплины

144 час(ов), 4 ЗЕТ

Форма промежуточной аттестации

Зачет

### *Б1.О.07.01 Математический анализ*

Цели освоения дисциплины

---

Целью преподавания дисциплины «Математический анализ» является: фундаментальная подготовка студентов в области математического анализа, овладение современным аппаратом математического анализа для дальнейшего использования математических знаний, умений и навыков в других дисциплинах и областях

---

Место дисциплины в структуре ОП

---

Дисциплина «Математический анализ» Б1.О.07.01 является дисциплиной обязательной части учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Изучение дисциплины «Математический анализ» основывается на базе знаний, умений и компетенций, полученных студентами в ходе освоения школьных курсов.

Требования к результатам освоения

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен использовать математические методы, необходимые для решения задач профессиональной деятельности; (ОПК-3)

Содержание дисциплины

Раздел 1. Теория пределов
Отображения и функции. Открытый интервал, круг, шар. Окрестности конечных и бесконечных точек. Открытые и замкнутые множества. Определение предела функции. Примеры. Свойства предела. Определение бесконечно малой функции. Бесконечно большие. Сравнение б.м. Таблица б.м Свойства непрерывных функций одной и нескольких переменных (без доказательств). Односторонние пределы. Разрывы и их классификация.
Раздел 2. Дифференциальное исчисление
Производная функции. Касательная. Частные производные. Теорема о приращении функции. Дифференциал. Таблица производных элементарных функций. Правила дифференцирования. Инвариантность первого дифференциала. Производная обратной и неявно заданной функции. Выпуклость функций одной переменной. Формула Тейлора. Теоремы Ферма, Ролля, Лагранжа, Коши. Правило Лопиталя. Экстремумы, монотонность и асимптоты функций одной переменной.
Раздел 3. Интегральное исчисление
Первообразная функции. Неопределённый интеграл и его свойства. Таблица интегралов и при-меры. Интегрирование по частям. Замена переменной в неопределённом интеграле. Интегри-рование рациональных функций. Определённый интеграл и его свойства. Теорема Барроу. Формула Ньютона-Лейбница. Несобственный интеграл. Замена переменной и интегрирование по частям в определённом интеграле. Применение интеграла (площадь, объём). Криволинейные интегралы. Двойной интеграл и его свойства Повторный интеграл. Замена переменных в двойном интеграле Формула Грина и её следствия (потенциальные поля).
Раздел 4. Дифференциальные уравнения
Дифференциальные уравнения (д.у.). Задача Коши. Теоремы существования и единственности решения задачи Коши. Поле направлений. Д.У. в полных дифференциалах. Однородные д.у. Линейные уравнения первого порядка. Уравнение Бернулли. Уравнения, допускающие понижение порядка. Линейные дифференциальные уравнения (л.д.у.). Линейно независимые решения однородного л.д.у. Вронскиан. Общее решение л.д.у. Метод вариации произвольных постоянных для нахождения частного решения. Л.д.у. с постоянными коэффициентами. Системы дифференциальных уравнений. Дифференциальные уравнения в частных производных.
Раздел 5. Ряды и ряды Фурье
Числовой ряд и его сумма. Свойства сходящихся рядов. Необходимый признак сходимости ряда. Теоремы сравнения. Достаточные признаки сходимости знакопостоянных рядов. Знакопеременные ряды. Абсолютная сходимость ряда. Признак Лейбница. Функциональные ряды. Степенные ряды; теорема Абеля. Дифференцирование и интегрирова-ние рядов. Ряды Тейлора и Маклорена. Решение д.у. с помощью степенных

рядов. Векторное пространство. Скалярное произведение. Ряд Фурье. Неравенство Бесселя и равенство Парсеваля. Ряд Фурье по тригонометрической системе функций. Теорема Дирихле. Различные формы ряда Фурье. Интеграл Фурье и преобразование Фурье.
Раздел 6. Операционное исчисление
Преобразование Лапласа и его свойства. Таблица оригиналов и изображений. Решение дифференциальных и интегральных уравнений методом преобразования Лапласа. Интеграл Дюамеля.

---

Общая трудоемкость дисциплины

360 час(ов), 10 ЗЕТ

Форма промежуточной аттестации

Экзамен

***Б1.О.07.02 Теория вероятностей и математическая статистика***

Цели освоения дисциплины

---

Целью преподавания дисциплины «Теория вероятностей и математическая статистика» является:

Целью преподавания дисциплины «Теория вероятностеи и математическая статистика» является:формирование фундамента подготовки будущих специалистов в области высшеи математики, а также, создавать необходимую базу для успешного овладения последующими специальными дисциплинами учебного плана.

---

Место дисциплины в структуре ОП

---

Дисциплина «Теория вероятностей и математическая статистика» Б1.О.07.02 является одной из дисциплин обязательной части учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Алгебра и геометрия»; «Математический анализ».

---

Требования к результатам освоения

---

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен использовать математические методы, необходимые для решения задач профессиональной деятельности; (ОПК-3)

---

Содержание дисциплины

---

Раздел 1. Случайные события
спытание. Событие. Полная группа событий. Классическое определение вероятности. Алгебра событий. Теорема о сложении и произведении вероятностей. Аксиоматическое определение вероятности. Геометрическая вероятность. Статистическая вероятность. Независимые события. Формула полной вероятности. Формула Байеса. Повторение испытаний. Схема Бернулли. Формула Пуассона. Локальная формула Муавра-Лапласа. Интегральная формула Муавра-Лапласа.
Раздел 2. Случайны величины
Дискретная случайная величина. Закон распределения вероятностей. Математическое ожидание, дисперсия и среднее квадратическое отклонение. Их свойства. Понятие о моментах распределения. Биномиальное распределение. Закон Пуассона. Непрерывная случайная величина. Функция распределения вероятностей. Плотность распределения вероятностей. Кривая распределения вероятностей. Математическое ожидание, дисперсия и среднее квадратическое отклонение непрерывной случайной величины. Закон равномерного распределения вероятностей. Показательное распределение. Закон Коши. Нормальный закон распределения вероятностей. Моменты нормального распределения. Правило трех сигм.
Раздел 3. Случайные векторы
Плотность распределения случайного вектора. Зависимые и независимые случайные величины. Числовые характеристики случайных векторов. Функция случайного аргумента. Равномерное распределение. Нормальный закон распределения двумерного случайного вектора. Неравенство Чебышёва. Сходимость случайных величин. Закон больших чисел. Центральная предельная теорема.
Раздел 4. Основы статистики
Основные понятия математической статистики. Выборка. Эмпирическая функция распределения. Полигон и гистограмма. Точечное и интервальное оценивание числовых характеристик и параметров распределения. Испытание статистических гипотез.

---

Общая трудоемкость дисциплины

144 час(ов), 4 ЗЕТ

Форма промежуточной аттестации

Экзамен

### *Б1.О.07.03 Алгебра и геометрия*

Цели освоения дисциплины

---

Целью преподавания дисциплины «Алгебра и геометрия» является:

обучение умению формулировать и решать алгебраические и геометрические в рамках задачи изучаемой специальности, умению творчески применять и самостоятельно дополнять свои знания.

---

Место дисциплины в структуре ОП

---

Дисциплина «Алгебра и геометрия» Б1.О.07.03 является дисциплиной обязательной части учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Изучение дисциплины «Алгебра и геометрия» основывается на базе знаний, умений и компетенций, полученных студентами в ходе освоения школьных курсов.

---

Требования к результатам освоения

---

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен использовать математические методы, необходимые для решения задач профессиональной деятельности; (ОПК-3)

---

Содержание дисциплины

---

Раздел 1. Комплексные числа.
Комплексные числа в алгебраической, тригонометрической и показательной формах. Действия с комплексными числами в разных формах. Формула Муавра. Степень и корень комплексного числа. Многочлены. Основная теорема алгебры. Разложение полинома на линейные множители.
Раздел 2. Матрицы. Определители. Системы линейных уравнений.
Матрицы. Основные понятия .Действия над матрицами. Определители . Свойства определителей.Вычисление определителей. Обратная матрица и ее свойства. . Ранг матрицы.Системы линейных уравнений. Матричная запись системы линейных уравнений.Теорема Кронекера-Капелли. Метод Гаусса.Метод Крамера.
Раздел 3. Векторная алгебра.
Векторы. Основные понятия.Операции над векторами. Ортонормированный базис на плоскости и в трехмерном пространстве. Скалярное, векторное, смешанное произведение векторов,их свойства.
Раздел 4. Аналитическая геометрия.
Линейные геометрические объекты и работа с ними. Кривые и поверхности второго порядка. Использование квадратичных форм

---

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

***Б1.О.07.04 Дискретная математика***

Цели освоения дисциплины

Целью преподавания дисциплины «Дискретная математика» является: формирование общетехнического фундамента подготовки будущих специалистов в области инфокоммуникационных технологий и систем связи, и создание необходимой базы для успешного овладения последующими специальными дисциплинами учебного плана.

Место дисциплины в структуре ОП

Дисциплина «Дискретная математика» Б1.О.07.04 является одной из дисциплин обязательной части учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Алгебра и геометрия».

Требования к результатам освоения

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен использовать математические методы, необходимые для решения задач профессиональной деятельности; (ОПК-3)

Содержание дисциплины

Раздел 1. Булева алгебра
Высказывания. Алгебра Буля. Основные логические функции. Таблица истинности. Свойства конъюнкции, дизъюнкции и отрицания. Нормальные формы. ДНФ, КНФ, СДНФ, СКНФ. Построе-ние сокращенных форм. Карты Карно. Полином Жегалкина. Суперпозиция функций. Таблица Поста. Теорема Поста. Полные наборы функций. Базисы. Релейно-контактные схемы. Логика предикатов
Раздел 2. Теория графов
Основные понятия теории графов. Связность графа. Пути, циклы. Эйлеровы и полуэйлеровы графы. Гамильтоновы и полугамильтоновы графы. Способы задания графов с использованием матриц. Сети и потоки в сетях. Теорема Форда-Фалкерсона. Алгоритма

Дейкстры. Деревья, основные свойства. Планарные графы. Раскраска графа.
Раздел 3. Множества. Бинарные отношения
Множества и бинарные отношения. Свойства бинарных отношений. Способы задания бинарных отношений. Отношение эквивалентности. Отношение порядка. Классы эквивалентности. Мощ-ность множества.
Раздел 4. Алгебраические структуры
Классификация алгебраических структур. Магма, полугруппа. Моноид. Группа. Таблица Кэли. Циклическая группа. Декартово произведение групп. Группа подстановок. Кольцо. Коммутативное кольцо. Идеал. Теория сравнений. Вычеты. Матрицы над полями. Системы линейных уравнений над полем. Малая теорема Ферма. Функция Эйлера. Теорема Эйлера. Характеристика кольца. Простой идеал. Евклидово кольцо. Кольцо многочленов. Теорема Безу. Расширение полей. Поле. Поле Галуа.

---

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

***Б1.О.07.05 Теория информации***

Цели освоения дисциплины

---

Целью преподавания дисциплины «Теория информации» является:
формирование у студентов теоретических знаний в области математических методов измерения количества аналоговой и дискретной информации, пропускной способности соответствующих каналов ее передачи в условиях наличия случайной деградации из-за помех, оптимальной обработки , а также формирования компетенций и практических навыков по умению расчета статистических характеристик источников информации, каналов передачи информации, владения методами синтеза и анализа эффективных кодов для сжатия информации, помехоустойчивых кодов для передачи по каналам и повышения достоверности, а также владения методами оптимального приема сигналов в условиях воздействия случайных помех.

---

Место дисциплины в структуре ОП

---

Дисциплина «Теория информации» Б1.О.07.05 является одной из дисциплин обязательной части учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем».
Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Дискретная математика»; «Информационные

технологии»; «Математический анализ»; «Теория вероятностей и математическая статистика».

---

Требования к результатам освоения

---

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

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

---

Содержание дисциплины

---

Раздел 1. Анализ линейных систем во временной и частотной области
Временные и частотные характеристики линейных сситем. Импульсная характеристика и частотная передаточная функция и связь между ними. Принципы анализа во временной области, свертка сигнала и импульсной характеристики. Спектральная плотность сигнала на выходе линейной системы.
Раздел 2. Математические модели случайных процессов. Прохождение случайных процессов через линейные цепи
Автокорреляционная функция случайного процесса. Применение импульсных и частотных характеристик для анализа линейных сис-тем.Связь АКФ с энергетическим спектром случайного сигнала, теорема Винера – Хинчина, интервал корреляции , белый шум. Узкополосные случайные процессы, распределение огибающей и фазы узкополосного случайного процесса. Нормальное распределение, связь корреляции и независимости выборок из нормального случайного сигнала.
Раздел 3. Информационные характеристики источников сообщений и каналов. Эн-тропия и коли-чество инфор-мации
Классификация источников сообщений и каналов. Три подхода к определению понятия “Количество информации”: комбинаторный, вероятностный, алгоритмический. Количество информации как мера снятой неопределенности. Информационные характеристики источников сообщений: эн-тропия - мера неопределенности состояний источника сообщений в среднем. Мера неопределенности Р. Хартли и К. Шеннона. Свойства энтропии дискретного источника. Априорная (безусловная) энтропия. Апостериорная (условная) энтропия дискретного источника и ее свойства.энтропия (безусловная, условная), количество информации, избыточность сообщения, производительность источника. Информационные характеристики каналов: скорость передачи ин-формации, максимальная скорость передачи информации (пропуск-ная способность канала), коэффициент использования канала. Информационные характеристики источников дискретных сообще-ний. Модели источников дискретных сообщений. Свойства эргоди-ческих источников. Избыточность и производительность дискретно-го источника. Двоичный источник сообщений. Информационные характеристики дискретных каналов. Идеальные (без помех) и реальные (с помехами) каналы. Скорость передачи и пропускная способность канала. Двоичный и “м - ичный" канал. Информационные характеристики источников непрерывных сооб-щений. Дифференциальная энтропия. Энтропия равномерного рас-пределения. Энтропия

гауссовского белого шума. Эпсилон - энтро-пия и эпсилон — производительность источника. Избыточность. Информационные характеристики непрерывных каналов. Модели непрерывных каналов. Скорость передачи информации и пропуск-ная способность. Сравнение пропускных способностей дискретных и непрерывных каналов.

Раздел 4. Основы теории передачи информации

Теоремы кодирования Шеннона для КС без помех и с помехами.Теоремы кодирования для дискретных каналов без памяти. Скорость передачи информации. Неравенство Фано (без доказательства). Обратная теорема кодирования для ДКБП. Прямая теорема кодирования для ДКБП (без доказательства). Предел Шеннона. Условная энтропия источника. Эпсилон-энтропия НС.

Раздел 5. Основы теории эффективного кодирования дискретных Сообщений. Кодирование источника ДС

Классификация кодов. Эффективное оптимальное кодирование как способ согласования информационных характеристик источника и канала. Кодирование источников без памяти (символы сообщений независимы) и с памятью (символы коррелированные между собой). Кодирование без потерь и с потерями. Кодовое дерево, префиксность кода и неравенство Крафта , равно-мерное кодирование, статистическое кодирование, кодирование по методу Шеннона-Фано, кодирование по методу Хафмена, теорема Шеннона о кодировании источника независимых сообщений, усло-вие оптимальности кодов. Словарное кодирование, алгоритм Лемпеля – Зива –Велча. Арифметическое кодирование.

Раздел 6. Основы теории помехоустойчивого кодирования. Кодирование канала Блочные линейные коды

Принципы корректирующего (помехоустойчивого) кодирования и декодирования с обнаружением и исправлением ошибок. Линейные систематические блочные коды. Код Хэмминга. Производящий полином, порождающая матрица. Проверочная матрица, фундаментальная матрица блочного линейного кода , понятие синдрома и синдромное декодирование блочных кодов.

Раздел 7. Сверточные коды и декодер максимального правдоподобия

Принципы работы сверточного кодера. Память кодера, кодовое ограничение, скорость кода,. Конечный автомат с памятью. Диаграмма состояний сверточного кодера, решетчатые диаграммы кодера Декодирование сверточных кодов .. Алгоритм декодирования по максимуму правдоподобия. Алгоритм деко-дирования Виттерби.

Раздел 8. Основы оптимального приёма дискретных и непрерывных сообщений

Содержание и классификация задач оптимального приёма ДС. Оптимальный приём ДС в КС с детерминированной и стохастиче-ской структурой. Обнаружение и различение ДС. Критерии опти-мального приёма ДС. Алгоритмы работы и структурные схемы оп-тимальных приёмников ДС в гауссовском КС. Синтез когерентного демодулятора ДС на фоне АБГШ. Согласованная фильтрация фи-нитных во времени сигналов. Импульсная характеристика и переда-точная функция согласованного фильтра.

Раздел 9. Потенциальная помехоустойчивость приёма.

Особенности передачи и приёма ДС в каналах с межсимвольной интерференцией, сосредоточенными по спектру и импульсными помехами. Критерии оптимального приёма НС. Отношение сигнал/помеха и вероятность ошибки при передаче ДС. Потенциальная помехоустойчивость систем передачи с различными видами модуляции.

Раздел 10. Методы многоканальной передачи и распределения информации.

Многопользовательская и многоканальная связь. Основы теории уплотнения и разделения сигналов в многоканальных системах связи. Многоканальная связь с временным, частотным, фазовым и кодовым уплотнением сигналов. Принципы создания

систем инфотелекоммуникаций на основе технологии ортогонального частотного мультиплексирования. Пространственное мультиплексированиев системах MIMO.

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

***Б1.О.08.01 Физика***

Цели освоения дисциплины

Целью преподавания дисциплины «Физика» является: фундаментальная подготовка студентов по физике; формирование навыков использования основных законов дисциплины к решению задач, связанных с профессиональной деятельностью; формирование у студентов научного мировоззрения, умения анализировать и находить методы решения физических проблем, возникающих в области, связанной с профессиональной деятельностью. Актуальность изучения учебной дисциплины в рамках основной профессиональной образовательной программы обусловлена необходимостью освоения студентами основных законов классической механики, электродинамики; освоение методов решения типичных физических задач, изучения методов проведения и обработки физического эксперимента, что позволяет формировать и развивать общепрофессиональные компетенции будущего специалиста.

Место дисциплины в структуре ОП

Дисциплина «Физика» Б1.О.08.01 является дисциплиной обязательной части учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Изучение дисциплины «Физика» основывается на базе знаний, умений и компетенций, полученных студентами в ходе освоения школьных курсов.

Требования к результатам освоения

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

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

Содержание дисциплины

Раздел 1. Механика
Кинематика материальной точки. Законы Ньютона. Закон изменения и сохранения импульса системы материальных точек. Момент импульса. Закон изменения и сохранения момента импульса системы материальных точек. Момент инерции твердого тела. Основное уравнение динамики вращательного движения. Работа силы. Консервативные силы. Связь консервативной силы и потенциальной энергии. Закон изменения и сохранения полной механической энергии.
Раздел 2. Электростатика
Электрический заряд. Закон Кулона. Электростатическое поле в вакууме. Вектор напряженности электрического поля. Силовые линии. Электростатическая теорема Гаусса. Потенциальный характер электростатического поля. Диэлектрики в электростатическом поле. Проводники в электростатическом поле. Электроемкость проводника и конденсатора. Энергия взаимодействия системы зарядов. Энергия заряженного конденсатора. Объемная плотность энергии электрического поля.
Раздел 3. Электрический ток
Электрический ток и его характеристики. Закон Ома. ЭДС. Закон Ома для неоднородного участка цепи.
Раздел 4. Магнитное поле
Магнитное поле. Сила Лоренца. Закон Био - Савара - Лапласа. Сила Ампера. Контур с током в магнитном поле. Магнитное поле в веществе. Виды магнетиков.
Раздел 5. Электромагнетизм
Явление взаимной индукции. Энергия магнитного поля. Вихревое электрическое поле. Ток смещения. Система уравнений Максвелла.
Раздел 6. Колебания и волны
Гармонические колебания. Свободные незатухающие гармонические колебания. Свободные затухающие колебания в механической системе и электрическом контуре. Сложение колебаний. Вынужденные колебания в механической системе и электрическом контуре. Волны и их характеристики. Интерференция волн. Стоячие волны. Скорость распространения упругой волны. Интенсивность волны. Элементы акустики. Эффект Доплера. Уравнение Даламбера для электромагнитной волны. Свойства электромагнитных волн. Интенсивность ЭМВ. Геометрическая оптика. Принцип Ферма.

Общая трудоемкость дисциплины

288 час(ов), 8 ЗЕТ

Форма промежуточной аттестации

Экзамен

### *Б1.О.08.02 Электротехника*

Цели освоения дисциплины

Целью преподавания дисциплины «Электротехника» является:

изучение основных понятий, определений и законов работы электрических устройств, которые широко используются во всех последующих специальных дисциплинах. Дисциплина «Теория электрических цепей» должна обеспечивать формирование фундамента подготовки будущих специалистов в области разработки средств связи, а также создавать необходимую базу для успешного овладения последующими специальными дисциплинами учебного плана. Она должна способствовать развитию творческих способностей студентов, умению формулировать и решать задачи изучаемой специальности, умению творчески применять и самостоятельно повышать свои знания. Эти цели достигаются на основе фундаментализации, интенсификации и индивидуализации процесса обучения путем внедрения и эффективного использования достижений науки и техники. В результате изучения дисциплины у студентов должны сформироваться знания, умения и навыки, позволяющие проводить самостоятельный анализ режимов работы электронных средств связи. Дисциплина является первой дисциплиной, в которой студенты изучают методы анализа электрических цепей. Она находится на стыке дисциплин, обеспечивающих базовую и специальную подготовку студентов. Изучая эту дисциплину, студенты впервые знакомятся с принципами работы электрических устройств. Приобретенные студентами знания и навыки необходимы для успешного овладения последующими специальными дисциплинами учебного плана.

---

Место дисциплины в структуре ОП

---

Дисциплина «Электротехника» Б1.О.08.02 является одной из дисциплин обязательной части учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Информатика»; «Математика»; «Физика».

---

Требования к результатам освоения

---

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования радиоэлектронной техники, применять физические законы и модели для решения задач профессиональной деятельности; (ОПК-4)
– Способен применять положения теории в области электрических цепей, радиотехнических сигналов, распространения радиоволн, кодирования, электрической связи, цифровой обработки сигналов для решения задач профессиональной деятельности; (ОПК-11)
– Способен применять технологии и технические средства сетей электросвязи; (ОПК-14)

Содержание дисциплины

Раздел 1. Основные понятия, определения и законы теории электрических цепей.
Электрическая цепь (ЭЦ), электрический ток, электрическое напряжение, энергия, мощность. Основы классификаций цепей. Линейные и нелинейные электрические цепи. Принцип суперпозиции. Модель и схемы ЭЦ. Активные и пассивные элементы ЭЦ. Основные понятия топологии ЭЦ. Законы Кирхгофа. Последовательное и параллельное соединение элементов ЭЦ.
Раздел 2. Анализ линейных резистивных ЭЦ.
Методы анализа ЭЦ: метод эквивалентных преобразований, метод наложения, метод токов ветвей, метод узловых напряжений, метод контурных токов. Основные теоремы ЭЦ: замещения взаимности, об эквивалентном генераторе.
Раздел 3. Анализ гармонических колебаний в ЭЦ.
Режим установившихся гармонических колебаний в ЭЦ. Мгновенная и средняя мощность, гармонические колебания в элементах ЭЦ. Символический метод анализа установившихся гармонических колебаний в ЭЦ. Комплексные сопротивления и проводимости пассивных элементов ЭЦ. Законы Ома и Кирхгофа в комплексной форме. Комплексная, средняя и реактивная мощности. Баланс мощностей. Цепи со взаимными индуктивностями. Особенности составления уравнений для цепей с магнитными связями.
Раздел 4. Частотные характеристики ЭЦ.
Комплексные передаточные функции ЭЦ. Амплитудно-частотные и фазо-частотные характеристики. Резонанс напряжений в последовательном колебательном контуре. Резонанс токов в параллельном колебательном контуре.
Раздел 5. Классический метод анализа переходных колебаний.
Установившиеся и переходные колебания в ЭЦ. Законы коммутации. Начальные условия. Переходные и свободные колебания в цепи с одним реактивным элементом. Переходные колебания в последовательном колебательном контуре.
Раздел 6. Операторный метод анализа колебаний в ЭЦ. Временные характеристики цепи.
Применение одностороннего преобразования Лапласа для анализа переходных колебаний в ЛЭЦ. Законы Ома и Кирхгофа для изображений колебаний. Схемы замещения реактивных элементов при нулевых и ненулевых начальных условиях. Алгоритм анализа переходных колебаний в ЛЭЦ операторным методом. Операторные передаточные функции устойчивых цепей и их свойства. Связь операторных передаточных функций с временными характеристиками ЭЦ.
Раздел 7. Аналоговые электрические фильтры.
Электрические фильтры. Определение, режимы нагрузок, классификация. Задача классического синтеза цепей, задачи аппроксимации и реализации. Методы аппроксимации по Тейлору, по Чебышеву. Полиномиальные фильтры нижних частот с характеристиками Баттерворта и с характеристиками Чебышева. Ослабление, порядок фильтра, передаточные функции. Реализация передаточной функции методом уравнивания коэффициентов. Реализация лестничных LCфильтров нижних частот. Применение реактансного преобразования частоты для расчета ФВЧ, ПФ и РФ. Принцип каскадно-развязанной реализации ARCфильтров
Раздел 8. Основы теории четырехполюсников
Четырехполюсники и их классификация. Уравнения передачи, параметры и матрицы параметров четырехполюсников. Соединения четырехполюсников. Характеристические и рабочие параметры. Режимы работы.

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

***Б1.О.08.03 Электроника и схемотехника***

Цели освоения дисциплины

Целью преподавания дисциплины «Электроника и схемотехника» является: формирование необходимого минимума специальных теоретических и практических знаний, обеспечивающих возможность понимать и анализировать процессы в радиоэлектронных цепях систем обработки сигналов.

Место дисциплины в структуре ОП

Дисциплина «Электроника и схемотехника» Б1.О.08.03 является одной из дисциплин обязательной части учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Теория электросвязи»; «Физика»; «Электротехника».

Требования к результатам освоения

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования радиоэлектронной техники, применять физические законы и модели для решения задач профессиональной деятельности; (ОПК-4)
– Способен применять положения теории в области электрических цепей, радиотехнических сигналов, распространения радиоволн, кодирования, электрической связи, цифровой обработки сигналов для решения задач профессиональной деятельности; (ОПК-11)
– Способен применять технологии и технические средства сетей электросвязи; (ОПК-14)

Содержание дисциплины

Раздел 1. Физические основы работы полупроводниковых приборов.

Электропроводность полупроводников. Электрические переходы. Смещение p-n-перехода. Ёмкость p-n-перехода. Пробой p-n-перехода. Полупроводниковые диоды.
Раздел 2. Биполярные и полевые транзисторы.
Структура и принцип действия биполярного транзистора. Способы включения биполярных транзисторов. Основные режимы работы транзистора. Физическая нелинейная модель транзистора и эквивалентные схемы. h-параметры биполярного транзистора. Основные параметры биполярных транзисторов. Транзисторы с инжекционным питанием. Транзистор с управляющим p-n-переходом. МДП (МОП) транзисторы. МДП-транзисторы со встроенным каналом. Способы включения полевых транзисторов. Полевой транзистор как четырехполюсник. МДП-структуры специального назначения. Нанотранзисторы.
Раздел 3. Электронные приборы с отрицательным дифференциальным сопротивлением. Компоненты оптоэлектроники.
Туннельный и обращенный диоды. Двухбазовый диод (однопереходный транзистор). Лавинный транзистор. Динисторы и тиристоры. Излучающие диоды. Фоторезисторы. Фотодиоды. Фототранзисторы. Оптроны. Дисплеи. Лазеры.
Раздел 4. Электронные усилительные устройства.
Общие сведения об усилителях электрических сигналов. Основные параметры и характеристики усилителей. Усилитель как четырехполюсник, параметры и эквивалентные схемы. Режимы работы усилительных каскадов. Цепи питания активных элементов. Межкаскадные связи. Усилительные каскады на биполярных транзисторах. усилительные каскады на полевых транзисторах.
Раздел 5. Усилители мощности и усилители постоянного тока.
Усилители с трансформаторным включением нагрузки. Безтрансформаторные двухтактные усилители. Усилители постоянного тока. Дифференциальный усилитель. Некоторые схемные решения, используемые в усилителях.
Раздел 6. Обратные связи в усилительных устройствах.
Виды ОС, коэффицент петлевого усиления и глубина ОС. Использование параметров четырехполюсника для описания усилителей с ОС. Влияние ОС на характеристики усилителя.
Раздел 7. Операционные усилители.
Общие сведения. Идеальный операционный усилитель. Основные параметры и характеристики операционных усилителей. Основные схемы включения ОУ и ООС.
Раздел 8. Генераторы электрических колебаний и электронные ключи.
Общие сведения. Генераторы гармонических сигналов. Кварцевые генераторы. Генераторы колебаний прямоугольной формы (мультивибраторы). Импульсные сигналы. Электронные ключи. Использование МОП-ключей в электронных устройствах с переключаемыми конденсаторами.
Раздел 9. Основы цифровой схемотехники электронных средств.
Основы теории логических (переключательных) функций. Комбинационные логические устройства. Триггеры и цифровые автоматы. Запоминающие электронные устройства.

---

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

***Б1.О.08.04 Теория электросвязи***

Цели освоения дисциплины

Целью преподавания дисциплины «Теория электросвязи» является:
изложение основных закономерностей обмена информацией на расстоянии, обработки, эффективной передачи и помехоустойчивого приёма в технических системах специального назначения и формирования фундаментальных знаний основ теории детерминированных и стохастических (случайных) аналоговых и цифровых сигналов и систем их формирования, преобразования, модуляции и обработки, основ математического моделирования современных систем и каналов передачи сигналов, методов аналоговой и цифровой модуляции сигналов для каналов с помехами, принципов и методов многоканальной передачи, хранения, распределения и приема дискретных и непрерывных сообщений, методов повышения энергетической и спектральной эффективности систем инфотелекоммуникаций базирующихся на фундаментальной теории временного, спектрального и корреляционного анализа сигналов, в том числе в радио и оптическом диапазоне, способствовать развитию творческих способностей студентов, умению вести поиск, анализ и систематизацию научно-технической информации в сфере будущей профессиональной деятельности, формулировать и решать задачи оптимизации систем специальной электрической связи, умению творчески применять и самостоятельно повышать свои знания в области инфотелекоммуникаций и специальной электрической связи.

Место дисциплины в структуре ОП

Дисциплина «Теория электросвязи» Б1.О.08.04 является одной из дисциплин обязательной части учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Теория информации».

Требования к результатам освоения

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

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

– Способен применять положения теории в области электрических цепей, радиотехнических сигналов, распространения радиоволн, кодирования, электрической связи, цифровой обработки сигналов для решения задач профессиональной деятельности; (ОПК-11)
– Способен применять технологии и технические средства сетей электросвязи; (ОПК-14)

---

Содержание дисциплины

---

Раздел 1. Общие сведения о системах электросвязи
Понятие информации, сообщения, сигнала. Модель системы передачи информации.Классификация сигналов в каналах связи. Исторические даты в истории связи и телекоммуникаций. ASCII (American Standard Code for Information Interchange). Телеграфный трёхрегистровый код МТК-2. Методы системного анализа телекоммуникаций. Временной и частотный анализ. Вероятностные подходы в построении и оптимизации систем связи. Статистическая теория обнаружения сигналов и оценки их параметров. Теория информации и кодирования.Сообщение и сигналы Радиотехнические цепи и сигналы: аналоговые, квантованые, дискретные, цифровые. Модель процесса коммуникации. Эталонная модель взаимодействия открытых систем (OpenSystemInterconnect - OSI). Основные преобразования информационных сигналов в цифровой связи. Форматирование: знаковое кодирование, дискретизация, квантование,ИКМ. Передача видеосигналов: NRZ, самосинхронизирующиеся форматы, фазовое кодирование, структура системы передачи информации, Классификация каналов передачи информации.
Раздел 2. Векторные и спектральные модели сигналов в инфотелекоммуникации
Векторные модели сигналов. Обобщенный ряд Фурье.Векторное представление сигнала. Понятие базиса, нормы, скалярного произведения сигналов, ортогональности сигналов, ортонормированного базиса сигналов. Алгебраическая структура пространства сигналов. Геометрическая структура пространства сигналов. Норма сигнала. Энергия сигнала. Метрика пространства сигналов. Скалярное произведение сигналов. Базисные сигналы. Обобщенный ряд Фурье.
Раздел 3. Спектры периодических и непериодических сигналов. Преобразование Фурье
Спектры периодических сигналов линейчатые и дискретные. Формы спектрального представления периодического сигнала. Спектры непериодических сигналов. Модель непериодического сигнала как предельного случая периодического сигнала , когда период повторения стремится к бесконечности. Физический смысл спектральной плотности сигнала. Математический и физический спектр непериодического сигнала. Прямое и обратное преобразование Фурье. Свойства преобразования Фурье.
Раздел 4. Спектрально-корреляционный анализ детерминированных сигналов в инфотелекоммуникации.
Энергетические модели сигналов. Корреляционные модели детерминированных сигналов. Распределение энергии в спектрах периодического и непериодического сигнала. Равенство Парсеваля и обобщенная формула Рэлея. Энергетический спектр сигнала. Распределение энергии в спектре вещественного непериодического сигнала. Эффективная ширина спектра сигнала. Автокорреляционная функция вещественного сигнала (АКФ) и ее свойства. Связь АКФ сигнала с его энергетическим спектром. АКФ периодического вещественного сигнала. Сигнал на выходе линейной системы. Частотная характеристика линейной системы. Свертка двух сигналов во временной и частотной области. Соотношение между сверткой и корреляцией.
Раздел 5. Концепция аналитического сигнала в радиотехнике и инфотелекоммуникации.

Аналитический сигнал и его спектр. Квадратурный и сопряженный сигналы. Спектральная плотность аналитического сигнала. Преобразование Гильберта во временной области. Преобразование Гильберта во частотной области. Преобразование Гильберта для гармонических сигналов. Понятие узкополосного квазигармонического сигнала. Формирование комплексной огибающей полосового сигнала. Синфазный и квадратурный сигналы. Реализация полосовых сигналов и квадратурной обработки. Квадратурная обработка вещественных узкополосных сигналов для выделения огибающей амплитуд и фазы огибающей.

Раздел 6. Дискретные сигналы в телекоммуникациях и специальной электрической связи.

Дискретизация аналогового сигнала по времени и квантование по уровню. Структура и разрядность АЦП. Шум квантования. Амплитудно-импульсная модуляция (АИМ), широтно-импульсная модуляция (ШИМ), время-импульсная модуляция (ВИМ), импульсно-кодовая модуляция (ИКМ). Математическая модель дискретизированного сигнала. Теорема Котельникова. Обобщенный ряд Фурье по системе базисных (ортогональных) функций Котельникова (ряд Котельникова) Восстановление аналогового сигнала по дискретным отсчетам. Спектральная плотность базисных функций Котельникова. Спектр дискретизированного сигнала. Преобразование Фурье для дискретизированного сигнала. Эффект наложения при дискретизации - элайсинг. Спектр дискретизированного сигнала при произвольной форме дискретизирующих импульсов, отличных о дельта-функций.

Раздел 7. Спектры дискретных сигналов. Дискретное преобразование Фурье. Алгоритмы БПФ.

Модель дискретного сигнала в частотной области. Дискретное преобразование Фурье. Поворачивающие множители и их свойства. Быстрое преобразование Фурье (БПФ) . Алгоритмы БПФ с прореживанием по времени. Алгоритмы БПФ с прореживанием по частоте. Применение БПФ для вычисления свертки. Синтез аналогового сигнала с использованием ОБПФ. Принципы ортогонального частотного мультиплексирования.

Раздел 8. Модуляция сигналов в радиотехнике, телекоммуникациях и специальной электрической связи.

Общие сведения о модуляции. Принципы модуляции сигналов. Несущий сигнал и информационный сигнал. Шкала частот гармонического несущего сигнала. Виды аналоговой модуляции, амплитудная модуляция, балансная модуляция, модуляция с подавлением несущей. Мгновенная полная фаза, мгновенная частота, угловая модуляция (ЧМ, ФМ, ОФМ). Временные и векторные диаграммы модулированных сигналов. Спектры модулированных сигналов. Демодуляция АМ сигнала. Амплитудное детектирование, квадратичное детектирование (нелинейное преобразование в режиме малого сигнала). Универсальный квадратурный модулятор и демодулятор. Формирование комплексной огибающей квадратурным модулятором.

Раздел 9. Принципы цифровой модуляции сигналов в системах специальной связи электрической.

Цифровая модуляция сигналов. Сигналы с дискретной амплитудной модуляцией. Дискретная частотная модуляция сигналов. Дискретная фазовая модуляция сигналов. Дискретная квадратурная модуляция сигналов.Технологии и виды цифровой модуляции в современных системах связи. Сигнальные созвездия, фазовая плоскость синфазной I и квадратурной Q компонент. Цифровая квадратурная модуляция. Код Грея. Решетчатая модуляция. Сигнальные-кодовые конструкции цифровых сигналов. Помехоустойчивость различных видов модуляции.

Раздел 10. Спектральная и энергетическая эффективность систем телекоммуникаций.

Цифровая модуляция сигналов. Сигналы с дискретной амплитудной модуляцией. Дискретная частотная модуляция сигналов. Дискретная фазовая модуляция сигналов.

Дискретная квадратурная модуляция сигналов.Технологии и виды цифровой модуляции в современных системах связи. Сигнальные созвездия, фазовая плоскость синфазной I и квадратурной Q компонент. Цифровая квадратурная модуляция. Код Грея. Решетчатая модуляция. Сигнальные-кодовые конструкции цифровых сигналов. Помехоустойчивость различных видов модуляции.

---

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

***Б1.О.09.01 Информатика***

Цели освоения дисциплины

---

Целью преподавания дисциплины «Информатика» является:
подготовка будущих специалистов, владеющих теоретическими знаниями, практическими навыками применения перспективных методов, современных средств информационных технологий и умением использовать эти знания для успешного владения последующих специальных дисциплин учебного плана.

---

Место дисциплины в структуре ОП

---

Дисциплина «Информатика» Б1.О.09.01 является дисциплиной обязательной части учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Изучение дисциплины «Информатика» основывается на базе знаний, умений и компетенций, полученных студентами в ходе освоения школьных курсов.

---

Требования к результатам освоения

---

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства; (ОПК-1)
– Способен создавать программы на языке высокого уровня, применять существующие реализации структур данных и алгоритмов; (ОПК-7)

---

Содержание дисциплины

Раздел 1. Модели решения функциональных и вычислительных задач
Моделирование как метод познания. Объект, субъект, цель моделирования. Цели, задачи, решаемые с помощью моделей. Эволюция и развитие Компьютеров. Архитектура ПК. Взаимодействие операционной системы с аппаратными средствами, драйверами, прикладным ПО, BIOS, виртуальными машинами. Загрузка ОС. Файловые системы. Жесткий диск. Типы файлов (исполняемые и т.п.) Многозадачность однопроцессорных ПК. Идея открытых исходных кодов.
Раздел 2. Технические средства реализации информационных процессов
Принципы аналогово-цифрового и цифро-аналогового преобразований. Кодирование информации. Передача аналоговых данных с помощью аналоговых сигналов. Передача цифровых данных с помощью аналоговых сигналов. Передача аналоговых данных с помощью цифровых сигналов. Передача цифровых данных с помощью цифровых сигналов
Раздел 3. Помехоустойчивые способы передачи информации
Теорема Котельникова. Дельта-модуляция. Принципы технологии 5G. Помехоустойчивое кодирование. Бит четности. Код Хемминга. Графическая интерпретация. Таблица Хемминга. Кодирование чисел. три подхода для кодирования отрицательных чисел.
Раздел 4. Принципы защиты информации, криптографии.
Способы обеспечения тайны передачи информации. Шифр Виженера. Шифрование про помощи случайных чисел. Шифрование с помощью псевдослучайных чисел. Требования для криптостойких хэш сумм. Алгоритм Диффи-Хэллмана. Электронная подпись. Лицензионный ключ.
Раздел 5. Программные средства реализации информационных процессов
Служебные программы, утилиты. Драйверы. Архиваторы. Антивирусные программы. Встроенные программы. Прикладное ПО. Прикладное ПО специального назначения. Среды программирования. Программные средства для мобильных устройств. Программные средства для периферийных устройств. ГОСТ Р ISO/МЭК 26300-2010 Информационная технология (ИТ).

---

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

### *Б1.О.09.02 Языки программирования*

Цели освоения дисциплины

---

Целью преподавания дисциплины «Языки программирования» является:
подготовка специалиста к деятельности, связанной созданием приложений в различных средах программирования. Ознакомление слушателей с основными возможностями языка программирования Python. Знания и практические навыки, полученные из курса «Языки программирования», используются обучаемыми при изучении естественнонаучных дисциплин, а также при разработке курсовых и дипломных работ.

Место дисциплины в структуре ОП

Дисциплина «Языки программирования» Б1.О.09.02 является одной из дисциплин обязательной части учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Информатика»; «Основы информационной безопасности».

Требования к результатам освоения

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства; (ОПК-1)
– Способен создавать программы на языке высокого уровня, применять существующие реализации структур данных и алгоритмов; (ОПК-7)

Содержание дисциплины

Раздел 1. Язык программирования Python
Введение в программирование и особенности языка. Основные условные операторы. Логические операторы. Основные структуры данных. Распространенные виды коллекций данных. Создание собственных простейших функций и их вызов.
Раздел 2. Объектно-ориентированное программирование
Основныt свойствf ООП (полиморфизм, наследование и инкапсуляция). Графика в Python, библиотека matplotlib. Работа с файлами. Возможности применения сторонних библиотек и модулей
Раздел 3. Архитектура виртуальной среды Cisco
Архитектура виртуальной среды Cisco
Раздел 4. Решение задач
Практическое применение языка программирования Python

Общая трудоемкость дисциплины

180 час(ов), 5 ЗЕТ

Форма промежуточной аттестации

Экзамен

***Б1.О.09.03 Технологии и методы программирования***

Цели освоения дисциплины

Целью преподавания дисциплины «Технологии и методы программирования» является:

изучение основных принципов, моделей и методов, используемых на различных этапах разработки программных продуктов.

Место дисциплины в структуре ОП

Дисциплина «Технологии и методы программирования» Б1.Б.14.03 является одной из дисциплин базовой части цикла учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Информатика»; «Языки программирования».

Требования к результатам освоения

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен создавать программы на языке высокого уровня, применять существующие реализации структур данных и алгоритмов; (ОПК-7)

Содержание дисциплины

Раздел 1. Основы объектно-ориентированного программирования.
Парадигмы программирования. Классификация языков программирования. Императивные языки программирования. Язык Си. Метод модульного программирования. Базовые понятия объектно-ориентированного программирования: объект, класс, инкапсуляция, полиморфизм, наследование. Класс в C++: сокрытие и доступность членов класса, конструктор, деструктор, перегрузка функций-членов класса, перегрузка операторов, друзья класса, использование механизма наследования, виртуальные функции. Элементы языка C++: стандартная библиотека языка C++, средства для работы с динамической памятью, консольный и файловый ввод/вывод с помощью объектовпотоков.
Раздел 2. Библиотеки языка C++
Библиотеки как средство реализации метода модульного программирования. Классификация библиотек по назначению, по составу. Примеры библиотек и условия их использования. Библиотека Qt: основные классы, структура простейшего приложения с графическим интерфейсом пользователя, простейшие элементы управления, обработка приложением событий, связанных с действиями пользователя, концепция «сигнал-слот». Инструментальная среда Qt Creator для создания приложения на основе Qt.

Раздел 3. Конструирование приложения с использованием базы данных
Основные понятия теории баз данных. Модели данных. Реляционные базы данных: термины, конструирование одно- и многотабличной базу данных. Примеры реляционных СУБД. СУБД SQLite. Язык SQL: основные команды, примеры запросов на выборку. Структура приложения, использующего базу данных. Средства организации работы приложения с базой данных. Классы Qt для взаимодействия с базой данных.
Раздел 4. Системы коллективной разработки программного обеспечения
Принципы организации группы разработчиков ПО. Распределение ролей в коллективе. Средства организации совместной работы. Системы контроля версий. Система Subversion: структура репозитория, основные команды управления данными, конфликты и способы из разрешения.
Раздел 5. Основы конструирования программных систем
Классический жизненный цикл программного обеспечения, характеристика его этапов. Стратегии конструирования ПО. Классификации ПО. Критерии качества ПО. Язык UML как средство анализа и проектирования ПО. Методы сбора и анализа требований к ПО. Концепция ПО. Спецификация и техническое задание. Средства анализа и проектирования ПО: DFD, ERD, STD, UML. Этапы проектирования. Типовые структуры ПО. Этапы и методы тестирования. Тестирование «черного ящика» и «белого ящика». Документирование программного обеспечения. Стандарты ГОСТ и ИСО в области конструирования ПО. Группа стандартов ЕСПД.

---

Общая трудоемкость дисциплины

144 час(ов), 4 ЗЕТ

Форма промежуточной аттестации

Экзамен

***Б1.О.09.04 Документоведение***

Цели освоения дисциплины

---

Целью преподавания дисциплины «Документоведение» является: формирование представления о важности документирования в профессиональной деятельности по обеспечению информационной безопасности. Документ здесь рассматривается и как объект защиты, и как объект хранения, и как средство описания способов и методов, применяемых при защите информации. Дается представление об электронных системах документооборота и вопросах обеспечения защищенного электронного документооборота на предприятии.

---

Место дисциплины в структуре ОП

---

Дисциплина «Документоведение» Б1.О.09.04 является одной из дисциплин обязательной части учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем».

Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Основы информационной безопасности».

---

Требования к результатам освоения

---

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

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

---

Содержание дисциплины

---

Раздел 1. Понятие телекоммуникационного права.
Субординация норм права. Конституционные основы деятельности в телекоммуникациях РФ.
Раздел 2. Система норм права регулирующих деятельность документооборота организации в РФ.
Структура контрольно-надзорных органов для коммерческих и государственных организаций. Основы внутреннего и внешнего документооборота организации.
Раздел 3. Федеральная связь РФ и ее состав
Федеральная связь РФ и ее состав. Сеть связи общего пользования. Выделенные сети связи. Технологические сети связи. Сети связи специального назначения. Государственное регулирование деятельности в области связи. Обязанности операторов связи в соответствии с федеральным законом РФ "О связи". Универсальные услуги связи. Подача жалоб и предъявление претензий и их рассмотрение. Место предъявления претензий. Основные положения Устава и Конвенции Международного союза электросвязи
Раздел 4. Информация, информационные технологии, в соответствии с законом РФ "Об информации, информационных технологиях и о защите"
Термины и определения, основные понятия рассматриваемые ФЗ № 149 "Об информации, информационных технологиях и о защите информации". Основные положения ФЗ.
Раздел 5. Персональные данные в соответствии с законом РФ "О персональных данных"
Основные понятия и положения рассматриваемые в ФЗ "О персональных данных".
Раздел 6. Правовые основы ограничения доступа к информации
Основные понятия и положения рассматриваемые в ФЗ "О Государственной тайне". Правовые основы защиты коммерческой тайны, СТРК, ГК РФ.
Раздел 7. Методы ограничения доступа к информации в ОС, в сетях связи.
Основные методы ограничения доступа к информации в ОС Windows, Unix. Матричная и мандатная модель уровня доступа. Основы ActiveDirectory в ОС WinServer.
Раздел 8. Нормативно-правовые основы электронной подписи в ГОСТах и СНИПах.
Основные понятия и положения рассматриваемые в ФЗ "Об электронной подписи». Основные положения ГОСТа Р 34.10-2012.
Раздел 9. Основы DLP-систем
Основные понятия и положения DLP-систем. Управление индексами и базами данных

компонентов DLP-системы на примере DLP «Контур информационной безопасности Searchinform» при помощи средств Searchinform DataCenter. Поиск по перехваченным документам при помощи приложения SearchinformClient.
Раздел 10. Основы электронного документооборота, этапы проектирования
Особенности проектирования и защиты электронного документооборота, основы защиты баз данных, основы защита корпоративного почтового документооборота.

---

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

***Б1.О.09.05 Информационные технологии***

Цели освоения дисциплины

---

Целью преподавания дисциплины «Информационные технологии» является: изучение техник и технологий обработки различных видов информации, теоретическое и практическое освоение информационных технологий и инструментальных средств для решения типовых общенаучных задач

---

Место дисциплины в структуре ОП

---

Дисциплина «Информационные технологии» Б1.О.09.05 является одной из дисциплин обязательной части учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Информатика».

---

Требования к результатам освоения

---

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

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

---

Содержание дисциплины

Раздел 1. Информационные технологии (ИТ) Введение в предмет.
Понятие «информационная технология» и её составляющие. Основные тенденции, проблемы и перспективы внедрения информационных технологий. Технологический процесс поиска, сбора и этапы обработки информации. Основные свойства ИТ. Теория формализации. Государственная программа цифровизации.
Раздел 2. Операционные системы.
Понятие операционной системы (ОС). Функции и классификация ОС. Системное и прикладное программное обеспечение (ПО). Структура обобщённой ОС. Архитектура ОС Linux, её основные компоненты. Файловые системы. Запуск ОС на виртуальных машинах (гипервизоры и виртуальные машины, обзор существующих решений, в том числе и свободного ПО). ОС Android и iOS. ОС: KaiOS, Sailfish OS (Аврора ОС). Архитектура, функции.
Раздел 3. Информационные технологии конечного пользователя
Прикладное программное обеспечение. Файловые менеджеры. Средства работы с жёсткими дисками, сервисное ПО. Резервное копирование, запись компакт дисков. Офисное ПО. Используемые государственные стандарты и форматы файлов для представления офисной информации. Текстовый процессор (например, свободное ПО LibreOffice Writer). Форматирование документов с использованием стилей. Автоматическое формирование оглавления и алфавитного указателя. Использование математических формул и рисунков в текстовых документах. Средства создания презентаций. Экспорт данных в pdf. Основы организации хранения данных с применением СУБД. Типы данных. Отношения между данными внутри БД. Нормализация. Язык запросов SQL. Выборка данных из нескольких таблиц. Объединяющие запросы. Свободное ПО – СУБД MySQL (PostgreSQL). Создание индексов. Создание резервной копии данных и восстановление. Доступ к СУБД из приложений (C++ и/или PHP). Доступ к СУБД из LibreOffice Base.
Раздел 4. Информационные технологии в глобальных, локальных и корпоративных сетях
Типовые структуры, классификация и принципы организации компьютерных сетей. Классификация аппаратных компонентов. Основы построения и структура информационно-вычислительных систем. Адресация на канальном и сетевом уровнях. Настройка сетевых интерфейсов в ОС. Взаимодействие программ через интернет сокеты.
Раздел 5. Развитие информационных технологий
Искусственный интеллект (ИИ). Разновидности интеллектуальных систем (рекомендательные системы и интеллектуальные системы поддержки принятия решений.) База знаний. Онтология в ИТ. Технология распознавания. Компьютерное зрение, обработка естественного языка, распознавание и синтез речи. Современные сферы применения технологий ИИ (нейропротезирование, нейроинтерфейсы, нейростимуляция, нейросенсинг и т.п.) Квантовые технологии. Современные направления производственных технологий. Цифровое проектирование и моделирование. Технологические задачи цифрового проектирования. 3D-моделирование в современном мире. Технология Digital Twin. Области применения цифровых двойников. Классификация «двойников». Системы PLM, MES. Компоненты робототехники и сенсорики. Сенсорика. Сенсоры, необходимые роботам. Датчики в робототехнике. Тенденции в сенсорике роботов. Технологии сенсорно-моторной координации и пространственного позиционирования. Технологии пространственного позиционирования. Сенсоры и обработка сенсорной информации.
Раздел 6. Технологии и средства глобальной сети интернет.
Веб-технологии. URL, DNS, Типы DNS-серверов. Глобальная сеть интернет и

предоставляемые ею услуги. Основы расширенного поиска технической информации в глобальной информационной сети интернет с использованием языка запросов. Системы управления контентом (CMS): WordPress, Joomla, Drupal, 1C-Bitrix, MODX. Технологии SEO продвижения сайтов в поисковых системах. SEO, Метрика, Web-визор.

---

Общая трудоемкость дисциплины

216 час(ов), 6 ЗЕТ

Форма промежуточной аттестации

Экзамен

***Б1.О.09.06 Аппаратные средства вычислительной техники***

Цели освоения дисциплины

---

Целью преподавания дисциплины «Аппаратные средства вычислительной техники» является:

формирование у студентов профессиональной компетенции в области вычислительной и микропроцессорной техники, что позволит им проектировать цифровые устройства любой степени сложности современными методами.

---

Место дисциплины в структуре ОП

---

Дисциплина «Аппаратные средства вычислительной техники» Б1.О.09.06 является одной из дисциплин обязательной части учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Дискретная математика»; «Информатика».

---

Требования к результатам освоения

---

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

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

---

Содержание дисциплины

---

Раздел 1. Введение

Предмет и задачи дисциплины. История создания вычислительной техники. Основные понятия и определения в области компьютерных систем (КС). Классификация КС. Этапы и основные тенденции развития архитектуры КС. Характеристика основных классов КС: персональные, портативные, рабочие станции, серверы, супер-ЭВМ и другие. Показатели качества и эффективности функционирования КС. Методы и средства оценки производительности КС. Методы и средства повышения надежности КС.
Раздел 2. Устройство персонального компьютера
Основные и дополнительные компоненты персонального компьютера.
Раздел 3. Центральный процессор
Архитектура и структура микропроцессора. Принципы функционирования микропроцессора. Классификации и основные характеристики микропроцессоров. Особенности микропроцессоров CISC, RISC, VLIW.
Раздел 4. Увеличение быстродействия процессора. Специализированные микропроцессоры.
Технологии выполнения команд в микропроцессоре: конвейеризация, динамическое выполнение, мультитредовое выполнение. Особенности архитектуры и структуры микропроцессоров: универсальных, сигнальных, сетевых, графических и др.
Раздел 5. Системная плата
Назначение и компоненты системной платы. Чипсеты системных плат. Внутренние и внешние интерфейсы системной платы.
Раздел 6. Оперативная память. Видеоадаптеры и звуковые адаптеры.
Назначение и характеристики оперативной памяти. Принципы работы оперативной памяти. Стандарты оперативной памяти. Назначение, стандарты и компоненты видеоадаптера. Интерфейсы и разъемы видеоадаптера. Принципы работы и характеристики видеоадаптера. Звуковые платы. Принципы функционирования и характеристики звуковой платы.
Раздел 7. Сетевые адаптеры. Накопители информации.
Адаптеры ЛВС. Модемы. Магнитные, оптические и магнитооптические устройства хранения данных. RAID-массивы. Внешние запоминающие устройства на флэш-памяти.
Раздел 8. Мониторы и сенсорные экраны.
Назначение, типы и основные характеристики мониторов. Принципы работы CKE и LCD мониторов, принципы работы плазменных и OLED мониторов. Сенсорные экраны графических планшетов и смартфонов.
Раздел 9. Устройства ввода информации. Устройства печати.
Устройства ввода: клавиатура, манипуляторы графической информации, сканеры. Устройства печати: матричные, струйные, лазерные принтеры, плоттеры.
Раздел 10. Заключение
Принципы построения, состав и назначение центров обработки данных (ЦОД). Современные и перспективные технологии построения ЦОД. Виртуализация аппаратных ресурсов ЦОД, грид- системы, облачные вычислительные инфраструктуры, виды облачных сервисов.

---

Общая трудоемкость дисциплины

180 час(ов), 5 ЗЕТ

Форма промежуточной аттестации

Экзамен

***Б1.О.09.07 Сети и системы передачи информации***

Цели освоения дисциплины

Целью преподавания дисциплины «Сети и системы передачи информации» является:

Изучение общих подходов к построению современных сетей связи, принципов взаимодействия использующихся технологий, сквозных решений для обеспечения качества обслуживания. Дисциплина «Сети и системы передачи информации» должна обеспечивать формирование фундамента подготовки студентов в области инфокоммуникаций, а также создавать необходимую базу для успешного овладения последующими специальными дисциплинами учебного плана. Она должна способствовать развитию творческих способностей студентов, умению формулировать и решать задачи изучаемой специальности, умению творчески применять и самостоятельно повышать свои знания.

Место дисциплины в структуре ОП

Дисциплина «Сети и системы передачи информации» Б1.О.09.07 является одной из дисциплин обязательной части учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Информатика»; «Основы информационной безопасности».

Требования к результатам освоения

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности; (ОПК-2)
– Способен использовать программные, программно-аппаратные и технические средства защиты информации при решении задач профессиональной деятельности; (ОПК-9)

Содержание дисциплины

Раздел 1. Современные сетевые технологии.
История сетевых технологий. Интернет. Что такое оконечное устройство. Операционная система сетевых устройств.
Раздел 2. Модель OSI.
Уровни модели. Инкапсуляция. Деинкапсуляция. Mac-адресация в сети Ethernet. Скорость и способы пересылки на коммутаторах. Маршруты и пути. Настройка интерфейсов.

Раздел 3. IP-адресация.
Структура IPv4. Сегментация сети. Типы IPv6 адресов.
Раздел 4. Сетевые пртоколы
Сообщения ICMP. Ping и traceroute. Протоколы TCP и UDP. Передача данных. Номера портов.
Раздел 5. Одноранговые сети.
Приложения вида клиент-сервер. Одноранговые приложения.
Раздел 6. Сервисы IPадресации.
Протоколы DNS. DHCP.
Раздел 7. Основы сетевой безопасности.
Уязвимости сетей. Виды атаки и методы защиты от них. Организация компьютерной сети предприятия. Приложения и протоколы, необходимые для построения сети предприятия.

---

Общая трудоемкость дисциплины

180 час(ов), 5 ЗЕТ

Форма промежуточной аттестации

Экзамен. Курсовой проект

***Б1.О.10.01 Основы информационной безопасности***

Цели освоения дисциплины

---

Целью преподавания дисциплины «Основы информационной безопасности» является:

формирование у обучаемых знаний в области теоретических основ информационной безопасности и навыков практического обеспечения защиты информации и безопасного использования программных средств в вычислительных системах.

---

Место дисциплины в структуре ОП

---

Дисциплина «Основы информационной безопасности» Б1.О.10.01 является одной из дисциплин обязательной части учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Алгебра и геометрия»; «Информатика»; «Физика».

---

Требования к результатам освоения

---

Процесс изучения дисциплины направлен на формирование следующих компетенций:

В соответствии с ФГОС:

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

---

Содержание дисциплины

---

Раздел 1. Введение в соревнования CTF.
История создания CTF. Виды соревнований CTF. Виды заданий CTF. Необходимые знания для решения задач.
Раздел 2. Обзор специализированного ПО для участия в соревнованиях CTF.
ПО для перехвата и анализа сетевого трафика. ПО для исследования структуры исполняемого файла. ПО для решения различных задач.
Раздел 3. Введение в вычислительные сети.
Модель OSI. Виды сетевого оборудования. Анализ сетевого трафика. Сетевые протоколы.
Раздел 4. Анализ скрытых вложений.
Определение стеганографии. Вложение в изображение. Атаки на стегосистемы.
Раздел 5. Реверс–инжиниринг.
Изучение метода обратной разработки. Использование инструментов для исследования структуры исполняемого файла.
Раздел 6. Цифровая криминалистика киберпреступлений.
Основные понятия Forensic (Computer forensic) . Виды инцидентов. Инструменты для решения задач forensic.
Раздел 7. Языки программирования в соревнованиях CTF.
Использование языков программирования для автоматического сбора информации в играх CTF.
Раздел 8. Основы криптоанализа.
Определение криптографии. Шифр цезаря. Шифр виженера. Шифр простой замены. Хэш-функции. Блочные и потоковые шифры. RSA. Атаки на шифры.
Раздел 9. Работа в UNIXподобных системах.
Файловые системы. Специфика типов файлов. Использование средств для удаленного подключения. Сервисы в UNIX системах.

---

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет. Курсовая работа

### *Б1.О.10.02 Организационное и правовое обеспечение информационной безопасности*

Цели освоения дисциплины

---

Целью преподавания дисциплины «Организационное и правовое обеспечение

информационной безопасности» является:

изучение студентами на основе действующего российского законодательства и нормативно-правовой базы организационно правового обеспечения информационной безопасности сетей и систем связи, приобретение знаний по организационному обеспечению информационной безопасности и формирование практических навыков работы по правовому обеспечению информационной безопасности.

---

Место дисциплины в структуре ОП

---

Дисциплина «Организационное и правовое обеспечение информационной безопасности» Б1.О.10.02 является одной из дисциплин обязательной части учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Документоведение»; «Основы информационной безопасности».

---

Требования к результатам освоения

---

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации; (ОПК-5)
– Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в процессе функционирования сетей электросвязи в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю; (ОПК-6)

---

Содержание дисциплины

---

Раздел 1. Правовое обеспечение информационной безопасности сетей и систем связи и пути его совершенствования. Задачи и функции правовой защиты информации
Цели, принципы, методы и средства правового обеспечения информационной безопасности РФ. Нормы законодательства РФ, регулирующие правовые отношения в сфере информационного обмена и обработки информации и позволяющие контролировать состояние безопасности сетей и систем связи, подключаемых к сети Интернет. Понятие конфиденциальности, целостности и доступности информации. Особенности разработки, производства и сертификации информационных систем, технологий и средств их обеспечения.
Раздел 2. Основные законодательные акты, регулирующие отношения, связанные с

правовой защитой и использованием интеллектуальной собственности. Защита информационных сетей и систем и прав на них
Общие положения Закона РФ “Об авторском праве и смежных правах”. Защита прав исполнителей, производителей фонограмм, организаций эфирного и кабельного вещания. Защита авторских и смежных прав. История развития законодательства о правовой охране программ для ЭВМ и баз данных. Порядок регистрации программ для ЭВМ и баз данных. Порядок передачи прав на использование программ для ЭВМ и баз данных по авторскому (лицензионному) договору. Понятие и виды информационных систем. Информационная война как целенаправленное информационное воздействие на информационные системы. Особенности правовой защиты информации в сетях и системах связи .
Раздел 3. Организационные источники и каналы утечки информации в сетях и системах. Силы, средства и условия организационной защиты информации
Национальные интересы РФ в информационной сфере и угрозы их безопасности. Информационная среда как предмет правового регулирования. Закон РФ “Об информации, информатизации и защите информации” как основа регулирования правоотношений в области информатизации. Правовые основы организации деятельности государственных органов, обеспечивающих информационную безопасность РФ. Основные направления совершенствования правового обеспечения информационной безопасности сетей и систем связи. Особенности раскрытия и расследования компьютерных преступлений. Информация как объект права. Понятие и виды защищаемой информации в сетях и системах связи. Основные термины в области правовой защиты информации.. Правовые задачи, принципы и функции защиты информации в сетях и системах связи. Закон РФ “Об информации, информатизации и защите информации” об основах правового режима информационных ресурсов (фондов) и порядке их использования.
Раздел 4. Особенности системы организационной защиты информации, составляющей государственную и коммерческую тайну
Требования к безопасности информации в сетях и системах связи. Защита инфокоммуникаций от несанкционированного доступа к информации. Структура и принципы функционирования современных сетей и систем связи. Проблемы обеспечения безопасности обработки и хранения информации в сетях и системах связи. Базовые этапы построения системы комплексной защиты сетей и систем связи. Управление системой защиты информации в сетях и системах связи.. Показатели защищенности от НСД к информации. Функции системы защиты по предупреждению угроз и устранению последствий их реализации. Классификация способов и средств комплексной защиты информации в сетях и системах связи. Компьютерные преступления. Политика безопасности. Модель мандатного доступа. Дискреционная политика. Матричная модель. Многоуровневые политики.
Раздел 5. Планирование процессов организационной защиты информации в сетях и системах Контроль функционирования системы организационной защиты информации
Сущность планирования как одной из основных функций управления системой организационной защиты информации в сетях и системах связи. Цели планирования. Оценка и анализ состояния системы ОЗИ как основа планирования. Стратегические и тактические планы. Разновидности планов; их содержание и форма. Методы планирования. Особенности программно-целевого планирования. Учет и отчетность по ОЗИ, как основа контроля. Объекты контроля. Методы контроля: анализ, наблюдение, проверка, сравнение, учет и др. Формы контроля: предварительный, текущий и заключительный. Технология контроля: выработка стандартов и критериев ОЗИ, сопоставление с ними полученных результатов и принятие необходимых корректирующих

действий. Выбор методов контроля, используемых на различных его этапах в зависимости от объектов контроля.

---

Общая трудоемкость дисциплины

144 час(ов), 4 ЗЕТ

Форма промежуточной аттестации

Экзамен

***Б1.О.10.03 Методы и средства криптографической защиты информации***

Цели освоения дисциплины

---

Целью преподавания дисциплины «Методы и средства криптографической защиты информации» является:

приобретение знаний в области основополагающими принципами криптографических методов и алгоритмов защиты информации, и навыков, которые можно применить при выполнении работ в качестве специалиста по информационной безопасности.

---

Место дисциплины в структуре ОП

---

Дисциплина «Методы и средства криптографической защиты информации» Б1.О.10.03 является одной из дисциплин обязательной части учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Математические основы защиты информации»; «Основы информационной безопасности».

---

Требования к результатам освоения

---

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен использовать методы и средства криптографической защиты информации при решении задач профессиональной деятельности; (ОПК-10)

---

Содержание дисциплины

Раздел 1. Введение в криптографию.
Основные определения. История криптографии. Классификация криптоалгоритмов.
Раздел 2. Математические основы криптографии.
Арифметика целых чисел. Модульная арифметика. Матрицы. Линейное сравнение. Алгебраические структуры. Поля Галуа. Структура генератора псевдослучайных последовательностей (ГПСП). Алгоритмы генерации псевдослучайных последовательностей Криптографические стойкие ГПСП. Тестирование ГПСП.
Раздел 3. Симметричная криптография.
Стандарт шифрования DES. Режимы работы алгоритма DES. Стандарт шифрования AES. Стандарт шифрования ГОСТ Р 34. 12-2015 (Магма и Кузнечик) Шифр одноразового блокнота. Принцип использования ГПСП при поточном шифровании. Шифр RC4.
Раздел 4. Криптосистема RSA.
Принцип работы современных асимметричных криптосистем. Криптосистема RSA. Криптосистема Эль-Гамаля. Криптосистема Рабина.
Раздел 5. Криптосистемы на основе метода эллиптических кривых.
Эллиптические кривые в вещественных числах, эллиптические кривые в полях Галуа, криптография эллиптической кривой, моделирующая криптосистему Эль-Гамаля.
Раздел 6. Криптографические хеш-функции.
Итеративные хеш-функции. Схема МеркеляДамгарда. Хеш- функции, основанные на блочных шифрах. Схема Рабина. Алгоритм безопасного хеширования SHA. Шифр Whirlpool. Российский стандарт хеширования ГОСТ Р 34.11-2012.
Раздел 7. Электронная цифровая подпись.
Алгоритм формирования электронной цифровой подписи (ЭЦП). Схема ЭЦП RSA. ЭЦП Эль-Гамаля. ЭЦП Шнорра. Стандарт цифровой подписи DSS. Схема ЭЦП эллиптической кривой. Российский стандарт ЭЦП ГОСТ Р 34.10- 2012.
Раздел 8. Алгоритмы безопасного распределения ключей.
Стандарт ANSI. X9.17. Методы хранения ключевой информации. Прямой обмен ключами между пользователями. Система «запрос-ответ». Алгоритм Ниидома-Шредера. Алгоритм Диффи-Хеллмана. Использование Центра распределения ключей. Инфраструктура PKI. Стандарт X.509. Система Kerberos.
Раздел 9. Основы современной стеганографии.
Цели стеганографии. Практическое применение стеганографии. Классификация алгоритмов стеганографии. Цифровые метки. Цифровые водяные знаки. Скрытая передача данных. Защита подлинности документов и авторских прав стеганографическими методами.
Раздел 10. Основы криптоанализа.
Методы криптоанализа. Криптоанализ блочных шифров. Частотный криптоанализ. Дифференциальный криптоанализ. Линейный криптоанализ. Интерполяционный криптоанализ. Методы криптоанализа, основанные на слабости ключевых разверток.

---

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

***Б1.О.10.04 Программно-аппаратные средства защиты информации***

Цели освоения дисциплины

Целью преподавания дисциплины «Программно-аппаратные средства защиты информации» является:

получение слушателями базовых теоретических знаний и практических навыков, необходимых для настройки защитных подсистем разграничения доступа, управления политиками безопасности, аудита и мониторинга состояния рабочих станций.

Место дисциплины в структуре ОП

Дисциплина «Программно-аппаратные средства защиты информации» Б1.О.10.04 является одной из дисциплин обязательной части учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Алгебра и геометрия»; «Дискретная математика»; «Информатика»; «Информационные технологии»; «Основы информационной безопасности»; «Основы информационной безопасности».

Требования к результатам освоения

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен использовать программные, программно-аппаратные и технические средства защиты информации при решении задач профессиональной деятельности; (ОПК-9)

Содержание дисциплины

Раздел 1. Корпоративная защита от внутренних угроз информационной безопасности.
Установка и настройка системы. Исследование (аудит) организации с целью защиты от внутренних угроз.
Раздел 2. Технологии анализа и защиты сетевого трафика.
Настройка сетевого окружения и компонентов систем. Защита локально-вычислительной сети предприятия.
Раздел 3. Технологии агентского мониторинга.
Технологии агентского мониторинга при помощи DLP-систем.
Раздел 4. Типовые аппаратные платформы АПКШ
Порядок ввода комплекса в эксплуатацию. Исследование АПКШ. Настройка Free BSD. Инициализация КШ.

Раздел 5. Правила фильтрации IPпакетов и правила трансляции.
Настройка правил фильтрации, разрешающих прохождение трафика между компьютерами из защищаемой сети и сети общего доступа. Настройка правила фильтрации, разрешающего прохождение трафика между компьютерами из внутренних сетей, защищаемых разными криптошлюзами. Настройка исходящего правила трансляции. Настройка входящего правила трансляции.
Раздел 6. Организация и управление VPN-соединениями
Организация L3VPN. VPN удаленного доступа. Мониторинг и диагностика системы защиты.
Раздел 7. Способы развертывания компонентов системы разграничения доступа.
Варианты установки компонентов системы разграничения доступа.
Раздел 8. Настройка и применение компонентов базовой защиты.
Организация управления системой защиты. Настройка и применение локальной аутентификации. Настройка аппаратной поддержки
Раздел 9. Настройка аудита в системе разграничения доступа.
Настройка регистрации событий на компьютерах. Хранение и очистка локальных журналов. Оповещения о событиях тревоги систем разграничения доступа.
Раздел 10. Реализация самозащиты в системах разграничения доступа.
Настройка систем в Dallas Lock. Настройка механизма контроля целостности. Централизованное ведение журналов. Управление подчинением защищаемых компьютеров серверу безопасности.
Раздел 11. Настройка и применение компонентов локальной защиты, Шифрование данных.
Управление криптографическими ключами пользователей. Настройка полномочного управления доступом. Настройка механизма дискреционного управления доступом. Управление доступом к съемным носителям информации. Использование криптоконтейнеров. Настройка теневого копирования и маркировки при контроле печати
Раздел 12. Сетевая защита в системах разграничения доступа.
Персональный межсетевой экран. Авторизация сетевых соединений. Защита от вирусов и вредоносного ПО. Средство обнаружения вторжений в системах разграничения доступа.
Раздел 13. Организация защиты средствами системы разграничения доступа.
Построение закрытого контура. Организация защиты средствами системы разграничения доступа согласно требованиям регуляторов.

---

Общая трудоемкость дисциплины

180 час(ов), 5 ЗЕТ

Форма промежуточной аттестации

Экзамен

### *Б1.О.10.05 Защита информации от утечки по техническим каналам*

Цели освоения дисциплины

---

Целью преподавания дисциплины «Защита информации от утечки по техническим каналам» является:

изучение студентами принципов построения и особенностям функционирования средств инженерно-технической защиты объектов инфокоммуникаций и включает в себя как методы и средства инженерно-технической защиты информации так и технические средства охраны объектов и помещений. В результате изучения дисциплины у студентов должны сформироваться знания, умения и навыки, позволяющие проводить самостоятельный анализ физических процессов, происходящих в инженерно-технических средствах защиты объектов, как изучаемых в настоящей дисциплине, так и находящихся за ее рамками.

---

Место дисциплины в структуре ОП

---

Дисциплина «Защита информации от утечки по техническим каналам» Б1.О.10.05 является одной из дисциплин обязательной части учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Дискретная математика»; «Защита в операционных системах»; «Информатика»; «Информационные технологии»; «Математический анализ»; «Методы и средства криптографической защиты информации»; «Организационное и правовое обеспечение информационной безопасности».

---

Требования к результатам освоения

---

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен использовать методы и средства криптографической защиты информации при решении задач профессиональной деятельности; (ОПК-10)
– Способен проводить специальные исследования на побочные электромагнитные излучения и наводки технических средств обработки информации (ПК-12)
– Способен проводить контроль защищенности информации от утечки за счет побочных электромагнитных излучений и наводок (ПК-13)

---

Содержание дисциплины

---

Раздел 1. Вводная лекция.
Термины и определения в области защиты информации от утечки по техническим каналам. Цели и задачи защиты информации от утечки информации по техническим каналам. Содержание и порядок изучения дисциплины.
Раздел 2. Технические каналы утечки информации, обрабатываемой СВТ.
Электромагнитные технические каналы утечки информации, обрабатываемой средствами

вычислительной техники (СВТ). Электрические и специально создаваемые технические каналы утечки информации, обрабатываемой средствами вычислительной техники (СВТ).
Раздел 3. Технические каналы утечки акустической (речевой) информации.
Характеристики речи. Классификация технических каналов утечки акустической (речевой) информации. Прямые акустические каналы утечки речевой информации. Акустовибрационные, акустооптический, акустоэлектрические и акустоэлектромагнитные каналы утечки речевой информации.
Раздел 4. Способы и средства защиты объектов информатизации от утечки информации по техническим каналам
Классификация способов и средств защиты объектов информатизации от утечки информации по техническим каналам. Экранирование и заземление технических средств. Системы пространственного электромагнитного зашумления. Способы и средства защиты объектов информатизации от утечки информации по цепям электропитания и заземления.
Раздел 5. Способы и средства защиты выделенных помещений от утечки речевой информации по техническим каналам.
Классификация способов и средств защиты выделенных помещений от утечки речевой информации по техническим каналам. Системы и средства виброакустической маскировки. Средства защиты ВТСС от утечки речевой информации по акустоэлектрическим каналам. Специальные технические средства подавления электронных устройств перехвата речевой информации.
Раздел 6. Методы и средства контроля защищенности информации, обрабатываемой СВТ.
Методы и средства контроля эффективности защиты информации, обрабатываемой СВТ. Порядок проведения контроля эффективности защиты СВТ от утечки информации, возникающей за счет ПЭМИН.
Раздел 7. Методы и средства контроля защищенности речевой информации от утечки по техническим каналам.
Методы и средства контроля выполнения норм защищенности речевой информации от утечки по техническим каналам. Порядок проведения контроля выполнения норм защищенности речевой информации от утечки по техническим каналам.
Раздел 8. Методы и средства выявления электронных устройств перехвата информации.
Классификация методов поиска электронных устройств перехвата информации. Методы и средства поиска электронных устройств перехвата информации средствами индикаторного типа. Методы выявления закладочных устройств с использованием сканирующих приемников и программно-аппаратных комплексов контроля
Раздел 9. Организация защиты информации от утечки по техническим каналам на объектах информатизации.
Порядок организации защиты информации от утечки по техническим каналам. Содержание технического задания на создание системы защиты информации от утечки по техническим каналам (СЗИУТК). Содержание технического проекта СЗИУТК. Аналитическое обоснование необходимости создания СЗИУТК. Организация аттестации объектов информатизации.

---

Общая трудоемкость дисциплины

144 час(ов), 4 ЗЕТ

Форма промежуточной аттестации

Экзамен

***Б1.О.10.06 Гуманитарные аспекты информационной безопасности***

Цели освоения дисциплины

Целью преподавания дисциплины «Гуманитарные аспекты информационной безопасности» является:

Сформировать у обучаемых целостное понимание социо-гуманитарных проблем информационной безопасности, связанных с процессом массовой компьютеризации всех сторон жизни и деятельности личности, общества и государства

Место дисциплины в структуре ОП

Дисциплина «Гуманитарные аспекты информационной безопасности» Б1.О.10.06 является одной из дисциплин обязательной части учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Основы информационной безопасности».

Требования к результатам освоения

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни (УК-6)
– Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности (УК-11)

Содержание дисциплины

Раздел 1. Место и роль проблем информационной безопасности в становлении современного информационного общества
Информация, информационные технологии и защита информации в информационном обществе. Нормативные документы в области информационной безопасности. Структура и задачи органов, обеспечивающих информационную безопасность.
Раздел 2. Личность, общество, государство и информационная безопасность.
Объективно значимые потребности личности, общества и государства в обеспечении их защищенности и устойчивом развитии в информационной сфере как национальные интересы РФ. Основные принципы обеспечение безопасности. Содержание деятельности по обеспечению безопасности. Информационная безопасность и стратегические национальные приоритеты РФ.

Раздел 3. Личность, её ценностные ориентации и информационная безопасность.
Личность в современном информационном пространстве. Ценностные ориентации личности и информационные технологии. Интернет и социальные сети. Этические кодексы профессиональной деятельности, связанной с компьютерными технологиями.
Раздел 4. Информационная безопасность и правонарушения в сфере информации, информационных технологий и защиты информации
Виды компьютерных правонарушений: использование вредоносного ПО, взлом паролей, кража персональных данных, фишинг, распространение противоправной информации. Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации.
Раздел 5. Интеллектуальная собственность и обеспечение её защиты в РФ
Понятие интеллектуальной собственности. Результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации, охраняемые в РФ как объекты интеллектуальной собственности. Защита интеллектуальной собственности в РФ.
Раздел 6. Интеллектуальная собственность
Понятие интеллектуальной собственности. Виды интеллектуального права: авторское право, смежные права, патентное право, прва на средства индивидуализации, право на секреты производства. Нарушение прав интеллектуальной собственности.
Раздел 7. Риски использования информационных технологий: вызовы и ответы
Понятие рисков в сфере информационных технологий. Риски, вызванные утечкой информации. Риски технических сбоев работы аппаратного и программного обеспечения, каналов передачи информации. Процессы минимизации ИТ-рисков

---

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

### *Б1.О.10.07 Основы управления проектами*

Цели освоения дисциплины

---

Целью преподавания дисциплины «Основы управления проектами» является: формирование совокупности теоретических знаний и практических навыков,связанные с основными источниками информации о проблемных ситуациях в профессиональной деятельности и подходами к критическому анализу этой информации; порядок принятия решений при возникновении проблемных ситуаций в профессиональной деятельности; умение организовывать работу коллектива(группы) для решения поставленных задач в сфере профессиональной деятельности и умение разрабатывать основные показатели технико-экономического обоснования соответствующих проектных решений

---

Место дисциплины в структуре ОП

Дисциплина «Основы управления проектами» Б1.О.10.07 является одной из дисциплин обязательной части учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Экономика».

Требования к результатам освоения

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен управлять проектом на всех этапах его жизненного цикла (УК-2)
– Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели (УК-3)
– Способен принимать обоснованные экономические решения в различных областях жизнедеятельности (УК-10)

Содержание дисциплины

Раздел 1. Сущность и содержание управления.
Законы, принципы и требования к управлению трудовым коллективом. Функции управления. Организация руководства трудовыми коллективами. Роль планирования в управленческой деятельности.
Раздел 2. Базовые концепции и модели процесса принятия решений.
Правила формулирования проблемы. Проблемная ситуация. Источники информации о проблемных ситуациях. Подходы к критическому анализу информации. Участники процесса принятия решений. Решения, принимаемые индивидуально. Решения, принимаемые группами людей. Методы, уровни и этапы принятия решений. Контроль принятых решений.
Раздел 3. Сущность и содержание управленческой деятельности руководителя.
Обобщенные задачи и функции руководителя. Влияние и власть, авторитет и лидерство, стили и методы работы руководителя. Этикет взаимоотношений руководителя и подчиненного. Социально-психологические характеристики рабочего коллектива и их учет.
Раздел 4. Организационная культура.
Поддержание организационной культуры, нравственных отношений и этикета взаимоотношений в коллективе. Конфликт в коллективе. Основные типы, причины и последствия конфликтов.
Раздел 5. Сущность и классификация проектов.
Отличительные характеристики и признаки проекта. Концепция и базовые понятия управления проектами: команда проекта, организационная структура. Роль менеджера проекта Управление проектом как искусство. Системный подход к управлению проектами. Основные ограничения проекта. Методы, показатели и критерии технико-

экономического обоснования проектных решений. Основные модели жизненного цикла проекта. Процессы, фазы и этапы жизненного цикла проекта, их основные характеристики. Международные и национальные стандарты управления проектами. Обзор Единой системы конструкторской документации и Единой системы программной документации в части постановки и выполнения научно-исследовательских и опытно-конструкторских работ.
Раздел 6. Методологии и процедуры управления проектами.
Функциональные области управления проектами: управление содержанием и объемом работ (управление целями проекта), управление временем (сроками) проекта, управление стоимостью проекта, управление качеством проекта, управление материально-техническим обеспечением (материальными ресурсами) проекта, управление человеческими ресурсами (персоналом) проекта, управление рисками проекта, управление информацией и коммуникациями в проекте, интеграционное управление проектом. Принципы деятельностного подхода к самообразованию, саморазвитию и самореализации. Способы самостоятельного получения новых знаний. Методы и средства самостоятельного решения задач.

---

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

### *Б1.О.10.08 Основы управления информационной безопасностью*

Цели освоения дисциплины

---

Целью преподавания дисциплины «Основы управления информационной безопасностью» является:
изучение вопросов управления информационной безопасностью. Дисциплина должна обеспечивать формирование фундамента подготовки будущих специалистов в области формирования моделей угроз, оценки рисков информационных инфокоммуникационных систем, формирование адекватных методов и средств обеспечения информационной безопасности, а также, создавать необходимую базу для успешного овладения последующими специальными дисциплинами учебного плана. Она должна способствовать развитию творческих способностей студентов, умению формулировать и решать задачи изучаемой специальности, умению творчески применять и самостоятельно повышать свои знания.

---

Место дисциплины в структуре ОП

---

Дисциплина «Основы управления информационной безопасностью» Б1.О.10.08 является одной из дисциплин обязательной части учебного плана подготовки

специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Основы информационной безопасности».

---

Требования к результатам освоения

---

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации; (ОПК-5)
– Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в процессе функционирования сетей электросвязи в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю; (ОПК-6)
– Способен проектировать защищенные телекоммуникационные системы и их элементы, проводить анализ проектных решений по обеспечению заданного уровня безопасности и требуемого качества обслуживания телекоммуникационных систем, разрабатывать необходимую техническую документацию с учетом действующих нормативных и методических документов, проводить подготовку исходных данных для технико-экономического обоснования соответствующих проектных решений; (ОПК-16)

---

Содержание дисциплины

---

Раздел 1. Оценка рисков информационной безопасности
Основные составляющие информационной безопасности. Угрозы информационной безопасности в информационныхсистемах. Основные определения и критерии, угрозы целостности и конфиденциальности.
Раздел 2. Стандарты управления информационной безопасностью
Государственные стандарты в области ИБ РФ. Оценочные стандарты в информационной безопасности. Оранжевая книга. Международный стандарт ISO/IEC 15408. Критерии оценки безопасностиинформационных систем. Стандарты управления информационной безопасностью BS 7799 и ISO/IEC 17799. Их основные положения Международный стандарт ISO/IEC 27001:2005 "Системы управления информационной безопасности. Требования"
Раздел 3. Принципы построения интегрированных систем информационной безопасности
Создание политик ИБ предприятия. Принципы обеспечения безопасности инфраструктуры. Принципы обеспечения безопасности периметра сети телекоммуникационной системы. Регулирование правил работы СКУД. Регулирование правил удаленного доступа средствами VPN. Контроль безопасности конечных устройств. Контроль безопасности IP-телефонии.
Раздел 4. Принципы организации аудита систем информационной безопасности
Основные техники проведения аудита систем ИБ. Разработка методики проведения аудита систем ИБ. Основные средства проведения аудита систем ИБ.

Раздел 5. Аудит инфраструктуры ИБ, интегрированных сервисов телефонии и беспроводного доступа
Основные механизмы и принципы проведения аудита ИБ инфраструктуры предприятия. Основные механизмы и принципы проведения аудита ИБ систем IP-телефонии, а также систем беспроводного доступа Wi-Fi
Раздел 6. Аудит систем удаленного и локального доступа
Основные механизмы и принципы проведения аудита ИБ СКУД предприятия, а также систем удаленного доступа с использованием технологий виртуальных частных сетей
Раздел 7. Введение в оценку и аудит ИБ путем выявления угроз ИБ «на лету»
Введение в «этическийхакинг». Основные принципы его организации. Составление плана проведения тестирования целевой системы (инфраструктуры). Отношение к законодательству и регуляторам. Составление отчета и рекомендаций на основе проведенного тестирования.
Раздел 8. Проведение комплекса процедур цифрового расследования в информационных и компьютерных системах
DigitalForensic. Расследование инцидентов. Утилиты для расследования инцидентов. Информация об истории посещения сайтов, кукисах, букмарках, скачанных файлах, заполненных формах, сохраненных логинах и т.д.
Раздел 9. Основные принципы построения SIEM
Средства визуализации элементов ИБ. Визуализация статистики по инцидентам ИБ. Комплексные системы мониторинга ИБ. Средства сбора отчетов и Logов. Основные принципы работы SIEM систем. Составление отчетов по ИБ.
Раздел 10. Управление информационной безопасностью на государственном уровне. Общие принципы и российская практика
Организационно-правовые формы управления безопасностью. Предпосылки развития государственного управления в сфере информационной безопасности. Общая методология и структура организационного обеспечения информационной безопасности на уровне государств. Общая политика России в сфере информационной безопасности. Структура органов государственной власти, обеспечивающих информационную безопасность в РФ.

---

Общая трудоемкость дисциплины

144 час(ов), 4 ЗЕТ

Форма промежуточной аттестации

Экзамен

### *Б1.О.10.09 Комплексная защита объектов информатизации*

Цели освоения дисциплины

---

Целью преподавания дисциплины «Комплексная защита объектов информатизации» является:
Формирование у студентов компетенций в области информационной безопасности и применения на практике методов и средств защиты информации.

---

Место дисциплины в структуре ОП

Дисциплина «Комплексная защита объектов информатизации» Б1.О.10.09 является одной из дисциплин обязательной части учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Защита в операционных системах».

Требования к результатам освоения

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен оценивать технические возможности, анализировать угрозы и вырабатывать рекомендации по построению элементов информационно-телекоммуникационной инфраструктуры с учетом обеспечения требований информационной безопасности; (ОПК-13)
– Способен проектировать защищенные телекоммуникационные системы и их элементы, проводить анализ проектных решений по обеспечению заданного уровня безопасности и требуемого качества обслуживания телекоммуникационных систем, разрабатывать необходимую техническую документацию с учетом действующих нормативных и методических документов, проводить подготовку исходных данных для технико-экономического обоснования соответствующих проектных решений; (ОПК-16)

Содержание дисциплины

Раздел 1. Введение в информационно - аналитическую деятельность комплексной безопасности (ИАДКБ)
Цели, задачи, объект, предмет информационно-аналитической деятельности комплексной безопасности (далее – ИАДКБКБ). Специфика ИАДКБ. Терминология. Особенности развития ИАДКБ в России. Основные принципы аналитической деятельности. Понятие информационно аналитических технологий.
Раздел 2. Первичная обработка информации.
Анализ модельной информации. Определение основных категорий и понятий. Выработка рабочей гипотезы. Конкретизация цели и задач исследования.
Раздел 3. Методика информационного поиска.
Поиск, отбор, экспресс-анализ первичных данных. Оптимизация поиска ресурсов удаленного доступа. Оптимизация поиска ресурсов удаленного доступа
Раздел 4. Анализ информативности источников.
Проблема активной фильтрации сообщений. Качественные характеристики информации. Режимы восприятия информации. Атрибуция сообщений
Раздел 5. Оценка полноты, непротиворечивости и достоверности информации. Технология создания аналитических документов
Критерии, параметры ограничения логической непротиворечивости и достоверности информации.

Раздел 6. Отчетные документы ИАДКБ.
Аналитический обзор и аналитическая записка: принципы составления. Информационная справка: принципы составления. Перспективы становления информационно-аналитической деятельности в сфере информационной безопасности.

---

Общая трудоемкость дисциплины

144 час(ов), 4 ЗЕТ

Форма промежуточной аттестации

Экзамен

***Б1.О.11.01 Математические основы защиты информации***

Цели освоения дисциплины

---

Целью преподавания дисциплины «Математические основы защиты информации» является:
изучение вопросов основ защиты информации в телекоммуникационных системах. В ходе прохождения данного курса студенты должны получить основные знания о математических основах построения криптографических алгоритмов, понятия о вычислительной сложности односторонних функций, используемых в криптографии, методах построения надежных систем защиты и о возможных атаках.

---

Место дисциплины в структуре ОП

---

Дисциплина «Математические основы защиты информации» Б1.О.11.01 является одной из дисциплин обязательной части учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Дискретная математика».

---

Требования к результатам освоения

---

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен формировать, внедрять и обеспечивать функционирование системы менеджмента информационной безопасности телекоммуникационных систем и сетей; (ОПК-9.1)

– Способен реализовывать комплекс организационных мероприятий по обеспечению информационной безопасности и устойчивости телекоммуникационных систем и сетей; (ОПК-9.2)
– Способен проводить мониторинг защищенности сетевых ресурсов и формировать отчеты по выявленным уязвимостям; (ОПК-9.3)

---

Содержание дисциплины

---

Раздел 1. Теория сложности и криптография
Теория сложности вычислений. Понятия простых и сложных алгоритмов. Машина Тьюринга, Классы P и NP(NPC).
Раздел 2. Теория чисел в криптографии
Арифметика целых чисел. Теория делимости и нахождении наибольшего общего делителя. Операции в модульной арифметике (арифметики над вычетами по модулю n). Применение модульной арифметики в криптографии.
Раздел 3. Простые числа в криптографии
Полиномиальные, экспоненциальные формулы. Числа Мерсена, Ферма. Псевдопростые числа. Тест Миллера.
Раздел 4. Принципы построения алгоритмов
Понятие алгоритма и его свойства. Способы описания алгоритмов. Свойства алгоритмов. Общие принципы построения алгоритмов. Основные алгоритмические конструкции
Раздел 5. Основные алгоритмы криптографии
Обзор самых распространенных алгоритмов шифрования и тенденций развития современной криптографии
Раздел 6. Формальные языки описания алгоритмов
Формальные языки. Классификация грамматик. Задача разбора. Метод рекурсивного спуска. Семантический анализ
Раздел 7. Основные криптографические протоколы
Основные протоколы криптографии. Свойства протокола. Виды криптографических протоколов. Протоколы конфиденциальной передачи сообщений. Протоколы аутентификации и идентификации. Протоколы распределения ключей. Протоколы электронной цифровой подписи. Протоколы обеспечения неотслеживаемости
Раздел 8. Эллиптические кривые
Криптосистемы на эллиптических кривых. Критерий простоты для эллиптических кривых. Разложение на множители на эллиптических

---

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

***Б1.О.11.02 Защита в операционных системах***

Цели освоения дисциплины

Целью преподавания дисциплины «Защита в операционных системах» является:

изучение вопросов защиты в операционных системах. Дисциплина "Защита в операционных системах" должна обеспечивать формирование фундамента подготовки будущих специалистов в области системного ПО, а также, создавать необходимую базу для успешного овладения последующими специальными дисциплинами учебного плана. Она должна способствовать развитию творческих способностей студентов, умению формулировать и решать задачи изучаемой специальности, умению творчески применять и самостоятельно повышать свои знания.

Место дисциплины в структуре ОП

Дисциплина «Защита в операционных системах» Б1.О.11.02 является одной из дисциплин обязательной части учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Информатика»; «Информационные технологии»; «Основы информационной безопасности»; «Теория вероятностей и математическая статистика».

Требования к результатам освоения

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен формировать, внедрять и обеспечивать функционирование системы менеджмента информационной безопасности телекоммуникационных систем и сетей; (ОПК-9.1)
– Способен реализовывать комплекс организационных мероприятий по обеспечению информационной безопасности и устойчивости телекоммуникационных систем и сетей; (ОПК-9.2)
– Способен проводить мониторинг защищенности сетевых ресурсов и формировать отчеты по выявленным уязвимостям; (ОПК-9.3)

Содержание дисциплины

Раздел 1. Внедрение и управление Windows Server
Различия версий Windows Server. Структура Windows Server. Развертывание Windows

Server.
Раздел 2. Введение в работу Active Directory Domain Services
Развертывание на основе ролеи. Развертывание серверов с конкретными ролями. Знакомство с доменными службами ActiveDirectory, реализация доменных служб AD, управление пользователями, группами, компьютерами. Понятие леса, домена. Протоколы аутентификации в домене: локальная аутентификация, протоколы сетевой аутентификации NTLM, Kerberos.
Раздел 3. Реализация локального хранилища в Windows Server
Многоуровневые пространства хранения. Создание пространств хранения. Ограничения пулов хранения. Создание виртуального диска.
Раздел 4. Файловый сервер и права доступа
Работа с iSCSI хранилищами. Общие папки NFS и CIFS. Модели контроля прав доступа к объектам файловой системы.
Раздел 5. Внедрение групповой политики
Архитектура механизма объектов групповой политики. Взаимосвязь групповой политики с объектами домена. Механизм распространения политики в домене. Защита Windows с помощью объектов групповой политики. Проектирование групповой политики с целью повышения уровня безопасности домена. Контроль учетных записеи, разрешения для фаилов и папок, блокировка учетной записи и политики паролей, детальные политики паролей, возможности аудита.
Раздел 6. Центр сертификации в Windows Server
Развертывание роли корневого центра сертификации. Структура цифрового сертификата. Процедура создания и проверки цифровой подписи. Применение цифровых сертификатов для повышения уровня безопасности домена. Установка и настройка Network Policy Server Role. Организация аутентификации сетевых устройств в домене. Внедрение модели AAA. Применение стека протоколов IPsec. Обзор встроенных средств мониторинга в операционной системе: диспетчер задач, мониторинг производительности, ресурсов, надежности и журналирование.
Раздел 7. Шифрование в файловой системе NTFS
Внедрение криптографических протоколов для защиты файлов.
Раздел 8. Управление службами удаленного рабочего стола
Развертывание роли удаленного рабочего стола. Управление удаленными приложениями. Организация сеанса тонкого клиента.
Раздел 9. Резервное копирование и обслуживание Windows Server
Использование Windows Server Backup для организации резервного копирования и восстановления системы. Создание резервной копии службы Active Directory.

---

Общая трудоемкость дисциплины

180 час(ов), 5 ЗЕТ

Форма промежуточной аттестации

Экзамен

***Б1.О.11.03 Криптографические протоколы***

Цели освоения дисциплины

Целью преподавания дисциплины «Криптографические протоколы» является: ознакомление студентов с основными понятиями теории криптографических протоколов; овладение основными идеями и методами современной теории криптографических протоколов; ознакомление студентов с основными криптографическими протокола распределения ключей, протоколами аутентификации, различными промежуточными и более развитыми протоколами; развитие навыка построения криптографического протокола из элементарных протоколов, и развития логического мышления в рамках этой задачи; овладение навыком разложения любого криптографического протокола на промежуточные с целью создания программного обеспечения, обслуживающего исполнение протокола.

Место дисциплины в структуре ОП

Дисциплина «Криптографические протоколы» Б1.О.11.03 является одной из дисциплин обязательной части учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Дискретная математика»; «Математические основы защиты информации»; «Математический анализ»; «Методы и средства криптографической защиты информации».

Требования к результатам освоения

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен формировать, внедрять и обеспечивать функционирование системы менеджмента информационной безопасности телекоммуникационных систем и сетей; (ОПК-9.1)
– Способен реализовывать комплекс организационных мероприятий по обеспечению информационной безопасности и устойчивости телекоммуникационных систем и сетей; (ОПК-9.2)
– Способен проводить мониторинг защищенности сетевых ресурсов и формировать отчеты по выявленным уязвимостям; (ОПК-9.3)

Содержание дисциплины

Раздел 1. Принципы построения систем шифрования

Введение в криптографию. Типы криптосистем. Модель системы шифрования. Способы шифрования. Влияние ошибок в криптограмме на дешифрование.
Раздел 2. Безусловностойкие криптосистемы
Необходимые и достаточные условия построения безусловно стойких криптосистем. Понятие расстояния единственности. Вывод формулы для расстояния единственности для произвольного шифра и ее анализ.
Раздел 3. Блочные шифры
Принципы построения блочных шифров. Шифры на основе схемы Фейстеля. Подстановочно перестановочные шифры. Методы криптоанализа блочных шифров: тотальный перебор ключей, анализ статистики криптограммы, линейный и дифференциальный. Модификации блоковых шифров. Стандарты шифрования AES, ГОСТ 3 34.12-15.
Раздел 4. Потоковые шифры
Принципы построения потоковых шифров. Линейный рекуррентный регистр и его свойства. Нелинейные узлы усложнения, используемые для построения потоковых шифров. Нерегулярное тактирование в потоковых шифрах. Основные методы криптоанализа потоковых шифров. Анализ шифра A5 стандарта GSM.
Раздел 5. Аутентификация сообщений
Модель системы аутентификации, классификация, характеристики эффективности. Безусловно стойкие системы аутентификации. Вычислительно-стойкие системы аутентификации. Способы построения ключевых хэш-функций. Системы аутентификации, на основе блочного шифра.
Раздел 6. Управление ключами в симметричных криптосистемах
Модель управления ключами. Этапы жизненного цикла ключа. Распределение ключей на основе ЦРК и доверенных каналов. Распределение ключей в интерактивном режиме с использованием ЦРК.

---

Общая трудоемкость дисциплины

180 час(ов), 5 ЗЕТ

Форма промежуточной аттестации

Экзамен

### *Б1.О.11.04 Основы построения защищенных компьютерных сетей*

Цели освоения дисциплины

---

Целью преподавания дисциплины «Основы построения защищенных компьютерных сетей» является:

дать представление студентам о современных угрозах информационной безопасности, протоколе AAA, технологиях построения межсетевых экранов и систем предотвращения вторжения, внедрения многофункционального устройства защиты нового поколения.

---

Место дисциплины в структуре ОП

Дисциплина «Основы построения защищенных компьютерных сетей» Б1.О.11.04 является одной из дисциплин обязательной части учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Основы информационной безопасности»; «Сети и системы передачи информации».

Требования к результатам освоения

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен формировать, внедрять и обеспечивать функционирование системы менеджмента информационной безопасности телекоммуникационных систем и сетей; (ОПК-9.1)
– Способен реализовывать комплекс организационных мероприятий по обеспечению информационной безопасности и устойчивости телекоммуникационных систем и сетей; (ОПК-9.2)
– Способен проводить мониторинг защищенности сетевых ресурсов и формировать отчеты по выявленным уязвимостям; (ОПК-9.3)

Содержание дисциплины

Раздел 1. Современные угрозы сетевой безопасности.
Обеспечение безопасности сетей. Векторы сетевых атак. Сетевые угрозы. Нейтрализация угроз.
Раздел 2. Обеспечение безопасности сетевых устройств.
Защита доступа к устройствам. Настройка безопасного административного доступа. Мониторинг устройств и управление ими.
Раздел 3. Аутентификация, авторизация и учет.
Назначение протокола AAA. Серверная аутентификация. Протоколы Radius, Tacacs+.
Раздел 4. Технологии межсетевого экрана.
Листы контроля доступа. Технологии межсетевого экрана. Зональные межсетевые экраны. Межсетевые экраны нового поколения.
Раздел 5. Системы предотвращения вторжений и аномалий.
Технологии IPS. Сигнатуры IPS. Внедрение системы IPS.
Раздел 6. Обеспечение безопасности локальной сети.
Безопасность оконечных устройств. Угрозы безопасности на канальном уровне.
Раздел 7. Внедрение виртуальных частных сетей.
Стек протоколов IPSec. Внедрение сетей IPSec VPN по схеме site-to-site.
Раздел 8. Внедрение многофункционального устройства защиты нового поколения.
Знакомство с межсетевым экраном нового поколения. Режимы работы. Конфигурирование.

Общая трудоемкость дисциплины

180 час(ов), 5 ЗЕТ

Форма промежуточной аттестации

Экзамен. Курсовая работа

***Б1.О.11.05 Основы построения сертифицированных защищенных баз данных РФ***

Цели освоения дисциплины

Целью преподавания дисциплины «Основы построения сертифицированных защищенных баз данных РФ» является:

Дать студентам методологию гибкой и безопасной разработки, построения и внедрения систем хранения данных, учитывающую выполнение требований законодательства РФ и противодействие угрозам безопасности информации.

Место дисциплины в структуре ОП

Дисциплина «Основы построения сертифицированных защищенных баз данных РФ» Б1.О.11.05 является одной из дисциплин обязательной части учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Основы информационной безопасности».

Требования к результатам освоения

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен формировать, внедрять и обеспечивать функционирование системы менеджмента информационной безопасности телекоммуникационных систем и сетей; (ОПК-9.1)
– Способен реализовывать комплекс организационных мероприятий по обеспечению информационной безопасности и устойчивости телекоммуникационных систем и сетей; (ОПК-9.2)
– Способен проводить мониторинг защищенности сетевых ресурсов и формировать отчеты по выявленным уязвимостям; (ОПК-9.3)

Содержание дисциплины

Раздел 1. Основные угрозы и средства защиты БД
Причины, виды, основные методы нарушения конфиденциальности в СУБД. Получение несанкционированного доступа к конфиденциальной информации путем логических выводов. SQL-инъекции. Средства обеспечения защиты информации в СУБД.
Раздел 2. Модели и методы обеспечения безопасности БД
Модели безопасности, применяемые при построении защиты в СУБД. Использование транзакции для изолирования действий пользователей. Блокировки. Ссылочная целостность, триггерная и событийная реализации правил безопасности. Особенности применения криптографических методов. Критерии защищенности БД и АИС.
Раздел 3. Разработка программ, осуществляющей хранение информации в БД
Основные понятия и классификация систем управления базами данных, общие требования к их разработке. Инфологическое проектирование, обоснование информационных объектов. Составление инфологической организованной модели. Создание таблиц.
Раздел 4. Работа с файлами БД на низком уровне
Понятие SQL Server. Ознакомление с архитектурой базы данных SQL Graph. SQL Server Компонент Service Broker.
Раздел 5. Подробный учёт существующих требований по ИБ
Основы подхода по проектированию БД. Модель нарушителя и угроз безопасности применительно к БД.
Раздел 6. Характерные уязвимости и атаки применимые к БД
«Отравление данных» или источников предоставления информации.
Раздел 7. Методы и способы нейтрализации угроз безопасности
Методы выявления ошибок и аномалий, воздействий на БД.
Раздел 8. Методы и способы резервирования информации
Методы и способы резервирования информации.
Раздел 9. Способы тестирования БД на уязвимости
Методы черного/серого/белого ящика. Фаззинг тестирование ПО с воздействием на БД.
Раздел 10. Заключительные положения и нюансы построения на практике
Перспективные технологии, в т.ч. ИИ и машинное обучение, подготовка верифицированных дата-сетов для них.

---

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

### *Б1.О.11.06 Методы оценки безопасности компьютерных систем*

Цели освоения дисциплины

---

Целью преподавания дисциплины «Методы оценки безопасности компьютерных систем» является:

предоставить студентам знания о методах и способах оценки безопасности

компьютерных систем. Рассмотреть общие критерии безопасности информационных технологий, оценочные уровни доверия. Методики оценки эффективности систем безопасности компьютерных систем. Оценка соответствия компьютерных систем требованиям по безопасности информации. Изучить инструментальные средства анализа защищенности компьютерных систем.

---

Место дисциплины в структуре ОП

---

Дисциплина «Методы оценки безопасности компьютерных систем» Б1.О.11.06 является одной из дисциплин обязательной части учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Защита в операционных системах».

---

Требования к результатам освоения

---

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен формировать, внедрять и обеспечивать функционирование системы менеджмента информационной безопасности телекоммуникационных систем и сетей; (ОПК-9.1)
– Способен реализовывать комплекс организационных мероприятий по обеспечению информационной безопасности и устойчивости телекоммуникационных систем и сетей; (ОПК-9.2)
– Способен проводить мониторинг защищенности сетевых ресурсов и формировать отчеты по выявленным уязвимостям; (ОПК-9.3)

---

Содержание дисциплины

---

Раздел 1. Методы и способы оценки безопасности компьютерных систем.
Изучение существующих методов и способов проведения оценки безопасности компьютерных систем. Недостатки и преимущества. Изучение алгоритмов проведения оценки безопасности компьютерных систем. Последовательность шагов. Результаты на каждом шаге.
Раздел 2. Безопасность информационных технологий.
Критерии оценки безопасности информационных технологий. Общая модель. Функциональные требования безопасности. Требования доверия к безопасности. Изучение комплекса стандартов ГОСТ ИСО/МЭК 15408. Введение в общую модель безопасности информационных технологий. Разбор функциональных требований безопасности. Разбор классов, семейств и компонентов безопасности. Разбор требований доверия к безопасности.
Раздел 3. Модели и оценка угроз безопасности информации в компьютерных системах.

Изучение методических рекомендаций по оценке угроз безопасности информации, утв. ФСТЭК России 05 февраля 2021 г. Разбор статичных отраслевых моделей угроз безопасности информации. Последовательность шагов. Определение рисков, негативных последствий, объектов воздействий, интерфейсов взаимодействия. Определение актуального нарушителя, его возможностей и мотивации. Изучение тактик, техник и способов реализации атак. Изучение существующих отечественных и зарубежных методик оценки эффективности систем безопасности компьютерных систем.
Раздел 4. Оценка соответствия компьютерных систем требованиям по безопасности информации.
Изучение форм оценки соответствия компьютерных систем требованиям по безопасности информации (184-ФЗ), аттестация объектов информатизации, декларация соответствия.
Раздел 5. Средства анализа защищенности компьютерных систем.
Изучение известных средств анализа защищенности компьютерных систем. Принципы работы.
Раздел 6. Инструменты для тестирования на проникновение в компьютерные системы.
Изучение известных инструментов для тестирования на проникновение в компьютерные системы на базе ОС Kali-Linux. Принципы работы. Изучение требований по оформлению отчетных материалов по результатам анализа защищенности и тестирования на проникновение в компьютерные системы.

---

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

***Б1.О.11.07 Администрирование средств защиты информации в компьютерных системах и сетях***

Цели освоения дисциплины

---

Целью преподавания дисциплины «Администрирование средств защиты информации в компьютерных системах и сетях» является:

предоставить студентам знания и навыки в объеме, достаточном для развертывания AAA-сервера на примере Cisco ISE и внедрению решений по контролю доступа в сети на основе стандарта 802.1X. Студенты получат практический опыт настройки наиболее эффективных решений для защиты от внешних угроз и обеспечения безопасности устройств, подключенных к сети.

---

Место дисциплины в структуре ОП

---

Дисциплина «Администрирование средств защиты информации в компьютерных системах и сетях» Б1.О.11.07 является одной из дисциплин обязательной части учебного плана подготовки специалитета по направлению «10.05.02

Информационная безопасность телекоммуникационных систем». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Основы информационной безопасности»; «Основы построения защищенных компьютерных сетей»; «Сети и системы передачи информации».

---

Требования к результатам освоения

---

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен формировать, внедрять и обеспечивать функционирование системы менеджмента информационной безопасности телекоммуникационных систем и сетей; (ОПК-9.1)
– Способен реализовывать комплекс организационных мероприятий по обеспечению информационной безопасности и устойчивости телекоммуникационных систем и сетей; (ОПК-9.2)
– Способен проводить мониторинг защищенности сетевых ресурсов и формировать отчеты по выявленным уязвимостям; (ОПК-9.3)

---

Содержание дисциплины

---

Раздел 1. Предотвращение угроз посредством служб идентификации.
Службы идентификации. Протокол 802.1 X и EAP.
Раздел 2. Основы системы Cisco ISE.
Обзор Cisco ISE. Механизмы аутентификации на Cisco ISE.
Раздел 3. Расширенные функции контроля доступа в сети.
Аутентификация на основе сертификатов пользователей. Использование SGA и применение технологии MACsec.
Раздел 4. Веб-аутентификация, гостевые порталы.
Знакомство с веб-аутентификацией. Знакомство с компонентами гостевых порталов. Настройка параметров гостевого доступа.
Раздел 5. Расширенные методы контроля доступа для периферийных устройств.
Posture-сервис. Сервис профилирования. Архитектура BYOD.
Раздел 6. Устранение неполадок в системе.
Устранение неполадок в работе системы контроля доступа.

---

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

***Б1.О.12 Моделирование систем и сетей телекоммуникаций***

Цели освоения дисциплины

Целью преподавания дисциплины «Моделирование систем и сетей телекоммуникаций» является:

получение навыков имитационного моделирования инфокоммуникационныхсетей и систем, а также изучение основ дискретно-событийного моделированиятелекоммуникационных протоколов и приложений.

Место дисциплины в структуре ОП

Дисциплина «Моделирование систем и сетей телекоммуникаций» Б1.О.12 является одной из дисциплин обязательной части учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Основы информационной безопасности».

Требования к результатам освоения

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

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

Содержание дисциплины

Раздел 1. Основы моделирования
Модель и моделирование. Классификация моделей. Модельное время. Этапы моделирования. Моделирование систем и сетей телекоммуникаций
Раздел 2. Работа с пакетом моделирования Riverbed Modeler
Введение. Установка и настройка
Раздел 3. Работа с пакетом моделирования Riverbed Modeler
Создание топологии сети
Раздел 4. Работа с пакетом моделирования Riverbed Modeler
Редактирование атрибутов объектов
Раздел 5. Работа с пакетом моделирования Riverbed Modeler
Сбор статистики
Раздел 6. Работа с пакетом моделирования Riverbed Modeler
Настройка параметров моделирования

Раздел 7. Работа с пакетом моделирования Riverbed Modeler
Просмотр и анализ результатов
Раздел 8. Работа с пакетом моделирования Riverbed Modeler
Генерация трафика
Раздел 9. Обработка результатов измерений
Виды измерений. Погрешности. Обработка результатов измерений. Погрешность косвенного измерения
Раздел 10. Обзор пакетов моделирования QualNet и ns-2
Введение. Создание топологии сети. Генерация трафика. Сбор статистики. Просмотр и анализ результатов

---

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

***Б1.О.13 Измерения в телекоммуникационных системах***

Цели освоения дисциплины

---

Целью преподавания дисциплины «Измерения в телекоммуникационных системах» является:
изучение теоретических основ метрологии, способов оценки точности (неопределенности) измерений и испытаний и достоверности контроля, принципов построения, структуры и содержания систем обеспечения достоверности измерений и оценки качества продукции, организации и правила проведения метрологической экспертизы, методов и средств поверки, калибровки и юстировки средств измерений

---

Место дисциплины в структуре ОП

---

Дисциплина «Измерения в телекоммуникационных системах» Б1.О.13 является одной из дисциплин обязательной части учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Моделирование систем и сетей телекоммуникаций».

---

Требования к результатам освоения

---

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен применять методы научных исследований при проведении разработок в области функционирования, развития и обеспечения информационной безопасности телекоммуникационных систем и сетей; (ОПК-8)
– Способен формулировать задачи, планировать и проводить исследования, в том числе эксперименты и математическое моделирование объектов, явлений и процессов телекоммуникационных систем, включая обработку и оценку достоверности их результатов; (ОПК-12)

---

Содержание дисциплины

---

Раздел 1. Введение в дисциплину.
Введение в дисциплину. Определение терминов: метрология, техническое регулирование, стандартизация, подтверждение соответствия, сертификация. Значение этих областей знания при разработке, производстве и эксплуатации телекоммуникационного оборудования и средств измерений.
Раздел 2. Нормируемые метрологические характеристики средств измерений.
Классификация средств измерений. Метрологические характеристики средств измерений, классы точности. Методы измерений. Эталоны единиц электрических величин.
Раздел 3. Погрешности измерений и неопределенности результатов измерении.
Классификация погрешностей. Систематические погрешности и методы их исключения. Случайные погрешности и их вероятностное описание. Неопределенности результатов измерений. Суммирование погрешностей. Погрешности косвенных измерений.
Раздел 4. Измерительные преобразователи переменного напряжения и тока.
Количественные характеристики переменного напряжения. Измерительные преобразователи переменного напряжения и тока. Вольтметры и анализаторы спектра.
Раздел 5. Аналоговые и цифровые осциллографы.
Наблюдение, измерение и исследование формы электрических сигналов. Классификация осциллографов. Аналоговые осциллографы, типовая структурная схема, метрологические характеристики. Генераторы линейной развертки (непрерывной, ждущей, задержанной). Режим внешней развертки. Осциллографические измерения. Цифровые осциллографы, структурная схема, принципы работы, метрологические характеристики, преимущества по сравнению с аналоговыми осциллографами.
Раздел 6. Цифровые измерения частоты, периода, интервалов времени.
Методы цифровых измерений частотновременных параметров сигналов: частоты, периода, интервалов времени, отношения частот. Структурные схемы электронносчетных частотомеров. Опорные генераторы. Источники погрешностей и их нормирование.
Раздел 7. Основные принципы технического регулирования. Отечественная, международная и межгосударственная стандартизация.
Правовые основы технического регулирования. Основные принципы и теоретическая база стандартизации. Виды стандартов. Отечественная и международная стандартизация в измерениях и технологических процессах. Роль стандартизации в повышении качества, безопасности и конкурентоспособности продукции, в развитии научно-технического и экономического сотрудничества.
Раздел 8. Подтверждение соответствия и сертификация.
Сертификация как форма подтверждения соответствия. Правовые основы, системы, схемы и этапы сертификации. Органы по сертификации и их аккредитация. Сертификация средств измерений, средств связи, радиоэлектронных средств.

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

## 2. Аннотации рабочих программ дисциплин (модулей) вариативной части

### *Б1.В.01 Введение в профессию*

Цели освоения дисциплины

Целью преподавания дисциплины «Введение в профессию» является:
формирование у студентов знаний об основных положениях ФГОС ВПО по направлению подготовки «Информационная безопасность», требованиях, предъявляемых к специалисту по информационной безопасности, а также актуальных проблемах защиты информации в современных условиях.

Место дисциплины в структуре ОП

Дисциплина «Введение в профессию» Б1.В.01 является дисциплиной части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Изучение дисциплины «Введение в профессию» опирается на знании дисциплин(ы) «Информатика».

Требования к результатам освоения

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен оценивать угрозы безопасности информации в компьютерных сетях (ПК-6)
– Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий (УК-1)

Содержание дисциплины

Раздел 1. История высшего образования в России и мире. История СПбГУТ Бонч-Бруевича.

История образования в мире. Первые университеты. Первые университеты в России. Жизнь и основные научные достижения проф. М.А.Бонч-Бруевича. История ЛЭИС – СПбГУТ. Структура факультета ИКСС. История, состав, основные достижения кафедры Защищенных систем связи.
Раздел 2. Направления подготовки бакалавров 10.05.02 Информационная безопасность.
Роль и место подготовки специалитета специализация №9 "Управление безопасностью телекоммуникационных систем и сетей". Структура учебного плана, содержание дисциплин. Анализ потребности в специалистах данного профиля на рынке труда.
Раздел 3. Криптография в истории. От древнего мира до настоящего времени.
История криптографии. История криптографии в России и СССР. Первые шифры. Библейский шифр, шифры Цезаря, Виженера, трафаретная система шифрования, шифры первой. Отечественной войны, шифры первой мировой войны, Энигма.
Раздел 4. История телекоммуникаций и компьютерных сетей.
История связи, компьютерные сети, возникновение Internet.
Раздел 5. Хакеры и проблемы информационной безопасности.
Феномен хакеров, причины появления, примеры. Актуальность вопросов информационной безопасности в современном мире.
Раздел 6. Дополнительные знания на кафедре ЗСС.
Сетевая академия Cisco, Направление CTF.
Раздел 7. Информационная война и промышленный шпионаж в современном мире.
Информационная война, исторические примеры, примеры из текущих новостей. Промышленный шпионаж в современном мире – примеры.
Раздел 8. Будущее Информационной безопасности.
Актуальность подготовки специалистов в области информационной безопасности.

---

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

### *Б1.В.02 Разработка защищенных сетевых приложений*

Цели освоения дисциплины

---

Целью преподавания дисциплины «Разработка защищенных сетевых приложений» является:

изучение основ семейства технологий, в основе которых используется программирование на языке Java, включая как собственно изучение назначения, синтаксиса, семантики и особенностей языка программирования Java, так и изучение методов проектирования информационных систем на Java.

---

Место дисциплины в структуре ОП

---

Дисциплина «Разработка защищенных сетевых приложений» Б1.В.02 является дисциплиной части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Изучение дисциплины «Разработка защищенных сетевых приложений» опирается на знании дисциплин(ы) «Алгебра и геометрия»; «Введение в профессию»; «Информатика»; «Информационные технологии»; «Математический анализ»; «Основы информационной безопасности»; «Языки программирования».

---

Требования к результатам освоения

---

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен создавать программы на языке высокого уровня, применять существующие реализации структур данных и алгоритмов; (ОПК-7)
– Способен анализировать угрозы безопасности информации программного обеспечения (ПК-9)
– Способен формулировать и обосновывать правила безопасной эксплуатации программного обеспечения (ПК-10)
– Способен осуществлять мероприятия по противодействию угрозам безопасности информации, возникающим при эксплуатации программного обеспечения (ПК-11)

---

Содержание дисциплины

---

Раздел 1. Основы разработки на Java.
Язык Java как средство программирования, преимущества, характерные особенности. Язык Java и Интернет. Отличия от C++. Типы данных, арифметические, логические, условные операторы и операторы цикла. Одномерные и многомерные массивы. Примеры простых программ.
Раздел 2. Основы объектно-ориентированного программирования.
Введение в концепцию объектно- ориентированного программирования, основные понятия, особенности реализации. Объявления классов. Основные компоненты класса: поля, методы, конструкторы. Вводится понятие наследования, полиморфизма. Обобщенные типы данных. Общие сведения об исключениях, обработка исключении с помощью конструкции try/catch/finally.Создание собственного исключения. Алгоритм обработки ошибок.
Раздел 3. Унифицированный язык объектно-ориентированного моделирования и документирования сложных систем.
Проектирование диаграмм моделирования процессов. Создание документации для совместной разработки программного обеспечения.
Раздел 4. Системы контроля версий.
Архитектура программного обеспечения для работы с изменяющимися данными. Использование систем контроля версии при совместной разработке.
Раздел 5. Организация потоков ввода-вывода.
Ввод-вывод данных в консольном и графическом режиме. Форматирование вывода, считывание ввода. Работа с потоками. Работа с текстовыми и бинарными файлами. Работа

с сетью TCP/IP. Многопоточное программирование.
Раздел 6. Создание графического интерфейса.
Создание окон, кнопок на окне, полей вывода, ввода, поля для рисования. Включение скроллинга. Менеджеры компоновки. Знакомство с методами обработки событии в Java: нажатие кнопки, движение мыши, нажатию кнопки на клавиатуре и д.р. с помощью интерфейсов.
Раздел 7. Структура байт кода.
Компиляция .java в .class., структура файла .class: заголовок; пул констант; объявления класса; поля методы; имена типов, методов и классов; исполняемые код. Примеры соответствия кода и байт кода.
Раздел 8. Технологии обеспечения безопасности.
Введение в основные механизмы встроенные в виртуальную машину JRE: загрузчики классов, верификация байт кода, диспетчеры полномочии, аутентификация пользователей, цифровые подписи, цифровые сертификаты, алгоритмы шифрования.
Раздел 9. Автоматизация сборки и развертывания проектов.
Организация сборки проекта: получение последней версии исходного кода, компиляция в исполняемый файл, выполнение тестов (модульные тесты, системные тесты, интеграционные тесты) скомпилированного кода, установка завершенного исполняемого файла, публикация результатов сборки.
Раздел 10. Основы разработки на Kotlin.
Язык Kotlin как модификация языка Java, преимущества, характерные особенности.

---

Общая трудоемкость дисциплины

144 час(ов), 4 ЗЕТ

Форма промежуточной аттестации

Экзамен. Курсовая работа

***Б1.В.03 Основы маршрутизации в компьютерных сетях***

Цели освоения дисциплины

---

Целью преподавания дисциплины «Основы маршрутизации в компьютерных сетях» является:
дать студентам углубленные знания в области построения компьютерных сетей, включая настройку протоколов DHCP, EtherChannel, FHRP.
Рассмотреть основные принципы построения беспроводных локальных сетей WLAN и методы их защиты. Рассмотреть концепцию VLAN и маршрутизации между VLAN, а также статическую маршрутизацию.

---

Место дисциплины в структуре ОП

---

Дисциплина «Основы маршрутизации в компьютерных сетях» Б1.В.03 является дисциплиной части, формируемой участниками образовательных отношений блока

1 учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Изучение дисциплины «Основы маршрутизации в компьютерных сетях» опирается на знании дисциплин(ы) «Введение в профессию»; «Основы информационной безопасности»; «Сети и системы передачи информации».

---

Требования к результатам освоения

---

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности; (ОПК-2)
– Способен оценивать угрозы безопасности информации в компьютерных сетях (ПК-6)

---

Содержание дисциплины

---

Раздел 1. Принципы коммутации. Базовая настройка устройств.
Принципы настройки протокола. Маршрут по умолчанию.
Раздел 2. Построение виртуальных локальных сетей. Маршрутизация между VLAN.
Понятие VLAN, транковых каналов. Основы маршрутизации между VLAN.
Раздел 3. Протокол связующего дерева STP.
Назначение. Принципы работы, выбор корневого коммутатора.
Раздел 4. Технология EtherChannel.
Характеристика технологии EtherChannel.
Раздел 5. Протоколы DHCPv4, SLAAC и DHCPv6.
Определение протоколов DHCP, SLAAC. Принципы функционирования.
Раздел 6. Основные понятие протоколов семейства FHRP.
Характеристика протоколов семейства FHRP.
Раздел 7. Принципы обеспечения безопасности в сети.
Протоколы AAA, 802.1X, атаки на протоколы ARP, DHCP. Способы защиты от атак на протоколы ARP, DHCP. Атаки на коммутаторы и способы защиты от этих атак. Атаки на VLAN. Настройка параметров безопасности на коммутаторах.
Раздел 8. Основные понятия беспроводных локальных сетей WLAN.
Понятие SSID. Обеспечение безопасности WLAN. Конфигурация WLAN.
Раздел 9. Принципы маршрутизации.
Понятие быстрой коммутации. Функции маршрутизатора, таблицы маршрутизации.
Раздел 10. Статическая маршрутизация.
Настройка статических маршрутов. Маршрут по умолчанию. Плавающие статические маршруты. Поиск и устранение неполадок, связанные со статическими маршрутами.

---

Общая трудоемкость дисциплины

144 час(ов), 4 ЗЕТ

Форма промежуточной аттестации

Экзамен

***Б1.В.04 Безопасность Astra-Linux***

Цели освоения дисциплины

---

Целью преподавания дисциплины «Безопасность Astra-Linux» является: изучение вопросов защиты операционных систем специального назначения. Дисциплина «Безопасность Astra-Linux» должна обеспечивать формирование фундамента подготовки будущих специалистов в области системного ПО, а также, создавать необходимую базу для успешного овладения последующими специальными дисциплинами учебного плана. Она должна способствовать развитию творческих способностей студентов, умению формулировать и решать задачи изучаемой специальности, умению творчески применять и самостоятельно повышать свои знания

---

Место дисциплины в структуре ОП

---

Дисциплина «Безопасность Astra-Linux» Б1.В.04 является дисциплиной части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Изучение дисциплины «Безопасность Astra-Linux» опирается на знании дисциплин(ы) «Введение в профессию»; «Дискретная математика»; «Защита в операционных системах»; «Информатика»; «Информационные технологии».

---

Требования к результатам освоения

---

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности; (ОПК-2)
– Способен формулировать и настраивать политики безопасности операционных систем (ПК-1)
– Способен противодействовать угрозам безопасности информации с использованием встроенных средств защиты информации операционных систем (ПК-3)

---

Содержание дисциплины

---

Раздел 1. История развития операционных систем семейства Unix
История разработки ОС Unix.Версии ОС. Стандарт POSIX. Развитие проекта GNU,

лицензия GNU GPL. Создание и развития дистрибутивов GNU/Linux. Анализ достоинств и недостатков различных операционных систем.
Раздел 2. Средства организации Единого Пространства Пользователей
Единое пространство пользователеи (ЕПП) – средства организации пользователеи в сети. Механизмы и службы организации ЕПП: механизмы NSS и PAM, службы каталогов LDAP, аутентификация Kerberos, служба AstraLinux Directory, шаблоны конфигурации, сценарии сессии пользователя. Администрирование домена.
Раздел 3. Защищенная графическая подсистема
Установка и настроика ОС. Системные компоненты: управления устроиствами, фаиловои системои, пользователями, перезагрузка и отключение. Системные сервисы и команды: сервисы, команды и графический интерфейс. Базовые сетевые службы.
Раздел 4. Модели разграничения доступа
Идентификация, аутентификация и авторизация. Дискреционное разграничение доступа: определения, Linux-привилегии, средства управления дирекционными правами доступа файлов и СУБД. Мандатное разграничение доступа: определения, привилегии, сетевое взаимодействие, средства управления мандатным доступом, средства управления привилегиями пользователей и процессов.
Раздел 5. Язык командного интерпретатора bash
Архитектура командной оболочки bash. Интерпретируемый язык bash, как средство разработки сценариев запуска, установки и управления сервисами операционной системы.
Раздел 6. Средства контроля целостности пакетов
Установка и удаление программ. Набор команд dpkg. Комплекса программ apt. Обновление программ и системы. Контроль целостности устанавливаемых пакетов.
Раздел 7. Взаимодействие с сетью
Подключение, настройка и управление сетевыми подключениями в операционных системах семейства Linux. Разграничение входящего и исходящего сетевого трафика.
Раздел 8. Защищенная система СУБД
Архитектуры современных баз данных. Организация баз данных в системах специального назначения. Мандатное разграничение доступом в СУБД.
Раздел 9. Резервное копирование и восстановление данных
Виды резервного копирования. Планирования резервного копирования. Инфраструктура для управления системой резервного копирования. Утилиты rsync и tar.
Раздел 10. Защита от отчуждаемого физического носителя
Контроль устройств компьютера и отчуждаемых носителей информации на основе централизованных политик, исключающих утечки конфиденциальной информации.

---

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

***Б1.В.05 Защита программ и данных***

Цели освоения дисциплины

Целью преподавания дисциплины «Защита программ и данных» является: теоретическая и практическая подготовка специалистов к деятельности, связанной с применением современных технологий анализа программных реализаций, защиты программ и программных систем от анализа и вредоносных программных воздействий.

Место дисциплины в структуре ОП

Дисциплина «Защита программ и данных» Б1.В.05 является дисциплиной части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Изучение дисциплины «Защита программ и данных» опирается на знании дисциплин(ы) «Аппаратные средства вычислительной техники»; «Введение в профессию»; «Защита в операционных системах»; «Информатика»; «Информационные технологии»; «Математические основы защиты информации»; «Технологии и методы программирования»; «Языки программирования».

Требования к результатам освоения

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен создавать программы на языке высокого уровня, применять существующие реализации структур данных и алгоритмов; (ОПК-7)
– Способен проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах (ПК-5)

Содержание дисциплины

Раздел 1. Введение в дисциплину "Защита программ и данных"
Общая информация о дисциплине, его целях. Организационные вопросы дисциплины. Методологические основы проведения исследования на программах и данных.
Раздел 2. Анализ программного кода и данных (Статический ручной)/(Динамический ручной)
Инструменты нарушителя, атакующего программы и данные статическим ручным способом. Инструменты нарушителя, атакующего программы и данные динамическим ручным способом. Способы защиты программ и данных от инструментов.
Раздел 3. Вредоносное программное обеспечение (как способ атаки на программы и данные)

Принцип действия вредоносного программного обеспечения. Способов защиты программ и данных от их заражения вредоносным программным обеспечением.
Раздел 4. Защита программного кода и данных (от статического анализа)/ (от динамического анализа)
Классификация способов защиты программ и данных от статического анализа. Классификация способов защиты программ и данных от динамического анализа. Способы защиты программ и данных от статического анализа.
Раздел 5. Возможный подход для анализа уязвимостей (как противодействия воздействиям, ослабляющим защиту программ и данных)
Возможные принципы взаимодействия уязвимостей в программном обеспечении. Способы защиты программ и данных от воздействия на них нескольких вредоносных программных объектов.
Раздел 6. Защита программ и данных в корпоративном программном обеспечении от социальных атак
Социальные атаки на корпоративное программное обеспечение. Способы защиты от социальных атак на корпоративное программное обеспечение.
Раздел 7. Защита программ и данных в частное программном обеспечении от социальных атак
Социальные атаки на частное программное обеспечение. Способы защиты от социальных атак на частное программное обеспечение.
Раздел 8. Классическое машинное обучение в защите программ и данных
Метод машинного обучения в аспекте анализа программного обеспечения. Применение методов машинного для защиты программ и данных.

---

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

### *Б1.В.06 Принципы организации глобальных вычислительных сетей*

Цели освоения дисциплины

---

Целью преподавания дисциплины «Принципы организации глобальных вычислительных сетей» является:

дать студентам знания в области построения глобальных сетей (WAN), включая концепцию качества обслуживания (QoS), принципы управления сетями, методы поиска и устранения неполадок в сети, технологии автоматизация сети, а также рассмотреть аспекты обеспечения безопасности в компьютерных сетях.

---

Место дисциплины в структуре ОП

---

Дисциплина «Принципы организации глобальных вычислительных сетей» Б1.В.06

является дисциплиной части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Изучение дисциплины «Принципы организации глобальных вычислительных сетей» опирается на знании дисциплин(ы) «Безопасность беспроводных локальных сетей»; «Основы информационной безопасности»; «Основы маршрутизации в компьютерных сетях»; «Сети и системы передачи информации».

---

Требования к результатам освоения

---

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности; (ОПК-2)
– Способен проводить инструментальный мониторинг качества обслуживания и анализ защищенности информации от несанкционированного доступа в телекоммуникационных системах и сетях в целях управления их функционированием; (ОПК-15)
– Способен оценивать угрозы безопасности информации в компьютерных сетях (ПК-6)

---

Содержание дисциплины

---

Раздел 1. Протокол динамической маршрутизации OSPF.
Принципы настройки протокола. Маршрут по умолчанию.
Раздел 2. Принципы обеспечения безопасности сети.
Уровни безопасности. Уязвимости IP.
Раздел 3. Принципы создания листов контроля доступа.
Назначение. Рекомендации по созданию. Типы листов.
Раздел 4. Трансляция сетевых адресов.
Характеристика технологии NAT. Преобразование адресов.
Раздел 5. Принципы работы WAN.
Назначение. Принципы работы. Подключение через Интернет.
Раздел 6. Принципы работы VPN и IPsec.
Технологии создания виртуальных частных сетей.
Раздел 7. Принцип работы QoS.
Качество передачи данных по сети. Характеристики трафика.
Раздел 8. Управление сетями .
Обнаружение устройств в сети. Проектирование сетей.
Раздел 9. Поиск и устранение неполадок в сети. Отладка сети.
Процедура поиска и устранения неполадок. Определение причин неполадок в компьютерных сетях.
Раздел 10. Автоматизация сети.
Обзор автоматизации. API-интерфейсы.

---

Общая трудоемкость дисциплины

144 час(ов), 4 ЗЕТ

Форма промежуточной аттестации

Экзамен

***Б1.В.07 Ассемблер в задачах защиты информации***

Цели освоения дисциплины

Целью преподавания дисциплины «Ассемблер в задачах защиты информации» является:

формирование у студентов теоретических знаний о принципах программирования микропроцессорных систем, способности самостоятельно разрабатывать программы на низкоуровневом языке программирования.

Место дисциплины в структуре ОП

Дисциплина «Ассемблер в задачах защиты информации» Б1.В.07 является дисциплиной части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Изучение дисциплины «Ассемблер в задачах защиты информации» опирается на знании дисциплин(ы) «Безопасность Astra-Linux»; «Введение в профессию»; «Основы информационной безопасности».

Требования к результатам освоения

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен создавать программы на языке высокого уровня, применять существующие реализации структур данных и алгоритмов; (ОПК-7)
– Способен анализировать угрозы безопасности информации программного обеспечения (ПК-9)
– Способен осуществлять мероприятия по противодействию угрозам безопасности информации, возникающим при эксплуатации программного обеспечения (ПК-11)

Содержание дисциплины

Раздел 1. Архитектура и система команд процессора.
Машинный язык и язык ассемблера. История процессоров Intel.
Раздел 2. Команды.
Команды обмена данных, арифметические команды. Применение логических команд.

Раздел 3. Работа со стеком и портами ввода/вывода.
Работа с битами. Применение макросов.
Раздел 4. Циклы.
Операторы цикла, функции.
Раздел 5. Работа с массивами.
Виды массивов. методы работы с массивами.
Раздел 6. Модульное программирование.
Составление программы из независимых блоков.
Раздел 7. Обфускация кода.
Приведение исходного текста или исполняемого кода программы к виду.
Раздел 8. Защита от реверс инжиниринга.
Защита программ от исследования, Антивирус из вируса.

---

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

***Б1.В.08 Проектирование защищенных телекоммуникационных систем***

Цели освоения дисциплины

---

Целью преподавания дисциплины «Проектирование защищенных телекоммуникационных систем» является:
освоения дисциплины является подготовка обучающихся к производственно-технологическому, организационно-управленческому, аналитическому и научно-исследовательскому видам деятельности

---

Место дисциплины в структуре ОП

---

Дисциплина «Проектирование защищенных телекоммуникационных систем» Б1.В.08 является дисциплиной части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Изучение дисциплины «Проектирование защищенных телекоммуникационных систем» опирается на знании дисциплин(ы) «Защита в операционных системах».

---

Требования к результатам освоения

---

Процесс изучения дисциплины направлен на формирование следующих компетенций:

В соответствии с ФГОС:

– Способен проектировать защищенные телекоммуникационные системы и их элементы, проводить анализ проектных решений по обеспечению заданного уровня безопасности и требуемого качества обслуживания телекоммуникационных систем, разрабатывать необходимую техническую документацию с учетом действующих нормативных и методических документов, проводить подготовку исходных данных для технико-экономического обоснования соответствующих проектных решений; (ОПК-16)
– Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни (УК-6)

---

Содержание дисциплины

---

Раздел 1. Понятие и структура проекта информационной системы(ИС)
Требования к эффективности и надежности проектных решений. Методы и средства проектирования ИС
Раздел 2. Основные компоненты технологии проектирования ИС
Выбор технологии проектирования ИС.
Раздел 3. Каноническое проектирование.
Стадии и этапы процесса проектирования ИС.
Раздел 4. Состав работ на предпроектной стадии, стадии технического и рабочего проектирования, стадии ввода в действие ИС.
Эксплуатация и сопровождение ИС
Раздел 5. Состав, содержание и принципы организации информационного обеспечения ИС.
Состав проектной документации
Раздел 6. Проектирование документальных и фактографических ИС
Анализ предметной области, разработка состава и структуры баз данных, проектирование логико-семантического комплекса.
Раздел 7. Технология проектирования ИС по архитектуре файл-сервер.
Особенности проектирования ИС по технологии файл-сервер. Оптимизация и администрирование ИС

---

Общая трудоемкость дисциплины

180 час(ов), 5 ЗЕТ

Форма промежуточной аттестации

Экзамен. Курсовой проект

### *Б1.В.09 Компьютерные вирусы*

Цели освоения дисциплины

---

Целью преподавания дисциплины «Компьютерные вирусы» является:
изучение вопросов основ защиты информации в глобальной сети на основе антивирусных решений компании ESETNOD32, одного из лидеров в этой области

разработки антивирусного программного обеспечения. Освоение студентами методов, способов и средств защиты компьютерных систем и сетей от вирусов.

---

Место дисциплины в структуре ОП

---

Дисциплина «Компьютерные вирусы» Б1.В.09 является дисциплиной части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Изучение дисциплины «Компьютерные вирусы» опирается на знании дисциплин(ы) «Защита программ и данных».

---

Требования к результатам освоения

---

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен создавать программы на языке высокого уровня, применять существующие реализации структур данных и алгоритмов; (ОПК-7)
– Способен устанавливать и настраивать антивирусные средства защиты информации в операционных системах (ПК-4)

---

Содержание дисциплины

---

Раздел 1. Классификация вирусов
Основные понятия и определения. Инструментарий для создания вирусов. Стиль «опасного» программирования. Состав вредоносных программ и команд.
Раздел 2. Вредоносное ПО
Основные понятия и определения. Инструментарий для создания вредоносного ПО.
Раздел 3. Жизненный цикл вредоносного ПО
Основы жизненного цикла вредоносного ПО.
Раздел 4. Механизмы проникновения
Внедрение и запуск на этапе самотестирования компьютера. Внедрение и запуск опасных программ с помощью «троянских» оболочек. Внедрение и запуск опасных команд с использованием ярлыков.
Раздел 5. Схемы заражения компьютерными вирусами
Основные виды вирусов и схемы их функционирования.
Раздел 6. Особености шифровальщиков
Изучение основ и особенностей шифровальщиков.
Раздел 7. Сетевые черви
Изучение основ и особенностей сетевых червей.
Раздел 8. Обфускация кода
Методы обфускации кода.
Раздел 9. Статический анализ
Применение статического анализа вирусов.

Раздел 10. Полиморфные вирусы
Основы полиморфных вирусов.

---

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

***Б1.В.10 Эксплуатация уязвимостей программного обеспечения***

Цели освоения дисциплины

---

Целью преподавания дисциплины «Эксплуатация уязвимостей программного обеспечения» является:
изучение студентом основных видов уязвимостей программного обеспечения, а также освоение основных методов и средств анализа и устранения уязвимостей программных реализаций.

---

Место дисциплины в структуре ОП

---

Дисциплина «Эксплуатация уязвимостей программного обеспечения» Б1.В.10 является дисциплиной части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Изучение дисциплины «Эксплуатация уязвимостей программного обеспечения» опирается на знании дисциплин(ы) «Безопасность Astra-Linux»; «Защита в операционных системах»; «Языки программирования».

---

Требования к результатам освоения

---

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен использовать программные, программно-аппаратные и технические средства защиты информации при решении задач профессиональной деятельности; (ОПК-9)
– Способен формулировать и обосновывать правила безопасной эксплуатации программного обеспечения (ПК-10)
– Способен осуществлять мероприятия по противодействию угрозам безопасности информации, возникающим при эксплуатации программного обеспечения (ПК-11)

---

Содержание дисциплины

Раздел 1. Анализ программных реализаций
Задача анализа программных реализаций. Метод экспериментов, статический метод, динамический метод. Принципы функционирования отладчиков. Факторы, ограничивающие возможности отладчиков. Методы поиска функций защиты в машинном коде: метод маяков, метод Step-Trace. Анализ потоков данных. Особенности анализа оверлейного кода, параллельного кода. Особенности анализа машинного кода в среде, управляемой сообщениями.
Раздел 2. Защита программ от исследования
Защита от дизассемблирования. Защита от отладки. Методы встраивания защиты в программное обеспечение. Методы обфускации (запутывания программного кода).
Раздел 3. Программные закладки
Понятие программной закладки. Классификация программных закладок. Модель «наблюдатель»: модульная структура закладки, организация информационного взаимодействия между клиентской и серверной частями. Модель «перехват»: перехватчики паролей первого, второго и третьего рода, защита от перехватчиков паролей первого рода в Windows, средства и методы перехвата сетевого трафика, перехват обращений пользователя к документам, электронной почте и веб-страницам. Модель «искажение»: применение программных закладок для несанкционированного повышения полномочий пользователя.
Раздел 4. Внедрение программных закладок
Предпосылки к внедрению программных закладок: уязвимости программного обеспечения, уязвимости политики безопасности, человеческий фактор. Методы внедрения программных закладок: маскировка под «безобидное» программное обеспечение, подмена, прямое и косвенное ассоциирование.
Раздел 5. Противодействие программным закладкам
Методы выявления программных закладок: сигнатурное и эвристическое сканирование, контроль целостности, мониторинг информационных потоков, изолированная программная среда, программные ловушки. Принципы построения политики безопасности, обеспечивающей высокую защищенность от программных закладок.
Раздел 6. Компьютерные вирусы как особый класс программных закладок
Бинарные вирусы Windows и Linux: структура, порядок инициализации, алгоритмы поиска и заражения жертвы. Сетевые вирусы: онлайн-вирусы, почтовые вирусы, IM-вирусы. Скриптовые вирусы: макровирусы, shell-вирусы, HTML-вирусы. Комбинированные вирусы. Средства и методы маскировки вирусов и противодействия антивирусному программному обеспечению: стелс-технологии, полиморфные преобразования кода.

---

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

***Б1.В.11 Основы стеганографии***

Цели освоения дисциплины

Целью преподавания дисциплины «Основы стеганографии» является: приобретение студентами знаний о важнейших разделах стеганографии и сформировать у студентов достаточно глубокие знания о теоретических основах стеганографии; современных методах стеганографии.

Место дисциплины в структуре ОП

Дисциплина «Основы стеганографии» Б1.В.11 является дисциплиной части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Изучение дисциплины «Основы стеганографии» опирается на знании дисциплин(ы) «Блокчейн и эллиптическая криптография»; «Криптографические протоколы»; «Методы и средства криптографической защиты информации»; «Основы криптографии с открытым ключом».

Требования к результатам освоения

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен использовать методы и средства криптографической защиты информации при решении задач профессиональной деятельности; (ОПК-10)
– Способен противодействовать угрозам безопасности информации с использованием встроенных средств защиты информации операционных систем (ПК-3)

Содержание дисциплины

Раздел 1. Области применения стеганографии
Определение цифровой стеганографии (СГ) в широком смысле. Собственно СГ и цифровые “водяные” знаки (ЦВЗ).Типичные покрывающие сообщения (ПС).Основные атаки на системы СГ и ЦВЗ.
Раздел 2. Простейшие системы СГ
Вложение в наименьшие значащие биты (НЗБ) с замещением и НЗБ с согласованием. Основные свойства СГ-НЗБ. Примеры систем с НЗБ (Jsteg,Outgiess,F5). СГ, использующие широкополосные сигналы (СГ-ШПС) и их свойства. Слепой и информированный декодеры.
Раздел 3. СГ для других покрывающих сообщений
Лингвистические, графические, Интернет СГ и их свойства.
Раздел 4. СГ стойкие к оптимальному статистическому обнаружению
Критерии секретности СГ. Относительная энтропия. Модельно обусловленные СГ.СГ на основе адаптивного квантования. СГ с сохранением статистики ПС. Слепой стегоанализ.

Раздел 5. Общие сведения о системах с ЦВЗ
Классификация систем ЦВЗ. Основные атаки на системы ЦВЗ. Критерии эффективности ЦВЗ. Виды ПС использующихся с ЦВЗ. Основные применения систем ЦВЗ
Раздел 6. Техника погружения и извлечения ЦВЗ устойчивых к случайному и преднамеренному удалению
Классификация систем ЦВЗ. Основные атаки на системы ЦВЗ. Критерии эффективности ЦВЗ. Виды ПС использующихся с ЦВЗ. Основные применения систем ЦВЗ (мониторинг рекламы ,идентификация пользователей доказательство прав собственности, аутентификация ПС).
Раздел 7. Особенности построения систем ЦВЗ для аудио и видео сигналов
ЦВЗ на основе использования явлений эхо и реверберации. Применение кепстральных методов в декодере. Защита от преобразований форматов. Основные методы построения систем ЦВЗ для видео ПС различных стандартов.

---

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

### *Б1.В.12 Защита информации в центрах обработки данных*

Цели освоения дисциплины

---

Целью преподавания дисциплины «Защита информации в центрах обработки данных» является:

формирование у обучаемых знаний в области комплексной защиты информации, которые дают представление о структуре и общем содержании концепции комплексной защиты информации в ЕИС ЦОД, и могут использоваться как основа для разработки унифицированных технологий защиты информации, обеспечивающих заданное качество защиты по всей совокупности показателей защищенности.

---

Место дисциплины в структуре ОП

---

Дисциплина «Защита информации в центрах обработки данных» Б1.В.12 является дисциплиной части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Изучение дисциплины «Защита информации в центрах обработки данных» опирается на знании дисциплин(ы) «Ассемблер в задачах защиты информации»; «Безопасность Astra-Linux»; «Безопасность IP-телефонии»; «Блокчейн и эллиптическая криптография»; «Введение в профессию»; «Защита в операционных системах».

Требования к результатам освоения

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен проектировать защищенные телекоммуникационные системы и их элементы, проводить анализ проектных решений по обеспечению заданного уровня безопасности и требуемого качества обслуживания телекоммуникационных систем, разрабатывать необходимую техническую документацию с учетом действующих нормативных и методических документов, проводить подготовку исходных данных для технико-экономического обоснования соответствующих проектных решений; (ОПК-16)
– Способен проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах (ПК-5)

Содержание дисциплины

Раздел 1. Введение в центры обработки данных (ЦОД)
Понятие центра обработки данных, структура ЦОД.
Раздел 2. Виртуализация и ЦОД
Настройка виртуальных машин, клонирование и создание шаблонов ВМ.
Раздел 3. Внедрение централизованного управления
Архитектура централизованного администрирования вычислительными ресурсами, хранилищами, подключением к сети и виртуальными машинами.
Раздел 4. Настройка и управление механизмами виртуальных сетей
Определение типов подключения виртуального коммутатора, настройка и просмотр стандартных конфигураций коммутаторов. Функциональные различия стандартных и распределенных коммутаторов.
Раздел 5. Настройка и управление механизмами виртуальных хранилищ
Рассмотрение различных концепций хранения данных. Изучение протоколов Fiber Channel, iSCSI, NFS, vSAN. Особенности файловой системы предназначенной для хранения файлов виртуальных машин.
Раздел 6. Управление механизмами защиты виртуальных машин
Создание шаблонов, мгновенных снимков виртуальных машин. Развертывание механизмов резервного копирования.
Раздел 7. Работа с ресурсами, мониторинг ресурсов
Управление виртуальными ресурсами, распределение ресурсов и мониторинг ЦОД.
Раздел 8. Развертывание и управления защищённым кластером ЦОД
Организация защищенного кластера для работы виртуальных машин используя механизмы динамического распределения ресурсов и высокой доступности.
Раздел 9. Управление жизненным циклом ЦОД
Управление жизненным циклом ЦОД для поддержания кластера в актуальном состоянии. Планирования обновлений, проверка совместимости.
Раздел 10. Введение в инфраструктуру облачных технологий
Описание компонентов инфраструктуры облака, процессов создания облачных услуг, управления облачными услугами.
Раздел 11. Механизмы обеспечения защиты в облаке
Рассказать об основных проблемах безопасности и защитных мерах в виртуализованном

ЦОД и облаке Рассмотреть основы контроля доступа и управлении идентификационными данными в облаке. Описать аспекты управления, риска и соответствия требованиям в облаке.

---

Общая трудоемкость дисциплины

180 час(ов), 5 ЗЕТ

Форма промежуточной аттестации

Экзамен

***Б1.В.13 Защита облачных вычислений и телекоммуникаций***

Цели освоения дисциплины

---

Целью преподавания дисциплины «Защита облачных вычислений и телекоммуникаций» является:

дать студентам представление о сетях следующего поколения, основных угрозах в облачных инфраструктурах и методах защиты данных в облачных инфраструктурах, а также рассмотреть методы построения программно-конфигурируемых сетей (SDN) и рассмотреть основные угрозы в сетях SDN.

---

Место дисциплины в структуре ОП

---

Дисциплина «Защита облачных вычислений и телекоммуникаций» Б1.В.24 является дисциплиной части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Изучение дисциплины «Защита облачных вычислений и телекоммуникаций» опирается на знании дисциплин(ы) «Администрирование средств защиты информации в компьютерных системах и сетях»; «Защита информации в центрах обработки данных»; «Основы построения защищенных компьютерных сетей»; «Технологии обеспечения информационной безопасности больших данных».

---

Требования к результатам освоения

---

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен применять методы научных исследований при проведении разработок в области функционирования, развития и обеспечения информационной безопасности телекоммуникационных систем и сетей; (ОПК-8)

– Способен формулировать и настраивать политики безопасности операционных систем (ПК-1)
– Способен устанавливать и настраивать антивирусные средства защиты информации в операционных системах (ПК-4)
– Способен проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах (ПК-5)
– Способен конфигурировать и контролировать корректность настройки программно-аппаратных средств защиты информации в компьютерных сетях (ПК-8)

---

Содержание дисциплины

---

Раздел 1. Введение в сети следующего поколения.
Переход на сети будущего. Проведено сравнение существующих сетей и сетей будущего.
Раздел 2. Безопасность и защита в облачных вычислениях.
Общие понятия облачных вычислений, проблемы обеспечения безопасности облачных вычислений, методология облачных вычислений.
Раздел 3. Виртуализация: Проблемы. Угрозы. Решения.
Проблемы виртуализации. Свойства и подходы в виртуализации, угрозы, решения.
Раздел 4. Принципы SDN. Протокол Openflow.
Программно-конфигурируемые сети, структура контроллера SDN, примеры конфигурации на решении компании Cisco Systems. Принципы конфигурирования протокола OpenFlow.
Раздел 5. Виртуализация сетей.
Принципы организации виртуальных сетей (на примере vSwitch от VMware), overlay сети.
Раздел 6. Виртуальные частные сети. Сетевой уровень. Транспортный уровень (протокол SSL/TLS).
Современные методы создания VPN, включая такие методы, как: IPsecVTI, динамические VTI, GETVPN, DMVPN, FlexVPN. Структура протоколов IPsec, IKEv.1 ив.2, приведены сравнительные характеристики всех современных методов построения VPN. Протоколы построения шифрованных туннелей трафика SSL/TLS. Основные уязвимости протоколов и способы борьбы с ними.
Раздел 7. Защита контроллера SDN.
Принципы организации защиты SDN контроллера, на примере компании Cisco Systems.
Раздел 8. Системы детекции/предотвращения вторжений и аномалий.
Системы предотвращения вторжений и аномалий (на примере ПО с открытым исходным кодом – Snort)
Раздел 9. Защита OpenStack.
Комплекс проектов свободного программного обеспечения, который может быть использован для создания инфраструктурных облачных сервисов и облачных хранилищ, как публичных, так и частных.
Раздел 10. Настройка продвинутого NAT, фаервола следующего поколения.
Конфигурация и принцип действия фаерволов следующего поколения (NGFW).
Раздел 11. Конфиденциальность облачных вычислений. Целостность облачных вычислений.
Основные угрозы и стратегии защиты облачных вычислений. Основные угрозы целостности данных и методы защиты от угроз в облачных вычислениях.

---

Общая трудоемкость дисциплины

216 час(ов), 6 ЗЕТ

Форма промежуточной аттестации

Экзамен

### *Б1.В.14 Основы проектирования систем защиты объектов информатизации*

Цели освоения дисциплины

Целью преподавания дисциплины «Основы проектирования систем защиты объектов информатизации» является:

Формирование у студентов компетенций в области информационной безопасности и применения на практике методов и средств защиты информации.

Место дисциплины в структуре ОП

Дисциплина «Основы проектирования систем защиты объектов информатизации» Б1.В.15 является дисциплиной части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Изучение дисциплины «Основы проектирования систем защиты объектов информатизации» опирается на знании дисциплин(ы) «Основы информационной безопасности».

Требования к результатам освоения

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

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

Содержание дисциплины

Раздел 1. Понятие и сущность информационной безопасности и защиты информации.
Необходимость и значимость нормативно-правового определения основных понятий. Понятие информационной безопасности (ИБ) и защиты информации. Основные компоненты безопасности государства и доминирующая роль ИБ. Становление и развитие понятия «информационная безопасность». Связь ИБ с информатизацией общества. Базовые уровни обеспечения ИБ и защиты информации.
Раздел 2. Основные угрозы информационной безопасности.

Классификация угроз безопасности по цели реализации угрозы, принципу, характеру и способу её воздействия. Особенности угроз воз-действия на объект атаки в зависимости от его состояния и используемых средств атаки. Основные методы и каналы несанкционированного доступа к информации в информационной системе (ИС). Базовые принципы защиты от несанкционированного доступа к информации в соответствии с нормативно-правовыми документами России. Задачи по защите ИС от реализации угроз.
Раздел 3. Система защиты информации.
Процесс развития средств и методов защиты информации. Этапы развития системы защиты информации в настоящее время. Комплексный подход к построению системы защиты информации. Системный подход к построению системы защиты информации. Цели задачи системы защиты информации. Этапы и порядок проведения работ по созданию системы защиты информации. Структура систем защиты информации на современном этапе. Методы (виды) обеспечения защиты информации.
Раздел 4. Обеспечение режима конфиденциальности при работе с защищаемой информацией.
Разрешительная (разграничительная) система доступа должностных лиц, работников к конфиденциальным сведениям, документам и базам данных. Доступ должностных лиц, работников к конфиденциальным сведениям, документам и базам данных. Обязанности должностных лиц, допущенных к сведениям, составляющим коммерческую тайну. Порядок предоставления (получения) конфиденциальной информации работникам сторонних организаций, государственным учреждениям.
Раздел 5. Контроль за соблюдением требований информационной безопасности и защиты информации.
Основные положения по осуществлению контроля, назначение, цель и задачи контроля. Основные мероприятия по осуществлению контроля. Порядок проведения проверки (контроля) наличия документов и иных носителей информации ограниченного доступа. Проведение служебного расследования по фактам утечки конфиденциальной информации, утраты носителей, содержащих такие сведения, а также по фактам грубых нарушений режима конфиденциальности.

---

Общая трудоемкость дисциплины

144 час(ов), 4 ЗЕТ

Форма промежуточной аттестации

Экзамен

### *Б1.В.15 Автоматизация и модернизация операционных систем сетевых устройств*

Цели освоения дисциплины

---

Целью преподавания дисциплины «Автоматизация и модернизация операционных систем сетевых устройств» является:
изучение вопросов защиты операционных систем.

---

Место дисциплины в структуре ОП

Дисциплина «Автоматизация и модернизация операционных систем сетевых устройств» Б1.В.15 является дисциплиной части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Изучение дисциплины «Автоматизация и модернизация операционных систем сетевых устройств» опирается на знании дисциплин(ы) «Безопасность Astra-Linux»; «Защита в операционных системах».

Требования к результатам освоения

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

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

Содержание дисциплины

Раздел 1. История развития операционных систем
История разработки ОС MSDOS, Windowsи Unix.Версии ОС. Стандарт POSIX. Развитие проекта GNU, лицензия GNUGPL. Создание и развития дистрибутивов GNU/Linux. Анализ достоинств и недостатков различных операционных систем.
Раздел 2. Основы взаимодействия с ОС GNULinux.
Сеанс работы пользователя в ОС: от регистрации в системе до выхода. Даются основы работы с интерфейсами командной строки и GUI. Основные понятия файловой системы: файл, каталог, дерево каталогов. Обсуждаются принципы размещения файлов в соответствии со стандартом FHS, приводится краткий обзор стандартных каталогов файловой системы EXT. Создание «песочницы» в ОС GNULinuxдля ограничений доступа к сервисам. Ведение системного журнала. Система управление пользователями и группами: создание, удаление, добавление в группы. Вводится понятие прав доступа как отношение субъектов системы (процессов) к объектам (файлам) и описывается мандатное управление доступом. Кроме того, описывается механизм подмены идентификатора, позволяющий в некоторых случаях строго ограниченным способом обходить запреты, устанавливаемые правами доступа. Организация сервисов, автозапуск сервисов, система управления сервисами. Описано семейство протоколов TCP/IP и их реализация в GNULinux, обосновано разделение сетевых протоколов на уровни и выделены задачи, решаемые на каждом из них. Приведены утилиты GNULinux для работы с сетью. Алгоритм обработки сетевого трафика. Настройка межсетевого экрана ОС GNULinux. Создание правил фильтрации трафика. Применение механизма SELinuxк обработке IP-пакетов. Организация и мониторинг Security-EnhancedLinux. Управление моделью безопасности SELinux: моды, контексты. Описание прав доступа к файлам и процессам.
Раздел 3. Система управления доступом в ОС MSWindows.

Основные компоненты ОС MSWindows. Модель операционной системы. Различие между клиентской и серверной версии. Системные процессы, драйвера, ядро. Вводится понятие реестр операционной системы. Управление сервисами и процессами. Система журналирования. Развертывание на основе ролей. Развертывание серверов с конкретными ролями.Знакомство с доменными службами ActiveDirectory, реализация доменных служб AD, управление пользователями, группами, компьютерами, внедрение групповой политики. Понятие леса, домена.
Раздел 4. Управление пользователями, группами и назначение прав доступа с использованием ActiveDirectory.
Контроль учетных записей, разрешения для файлов и папок, блокировка учетной записи и политики паролей, детальные политики паролей, возможности аудита, функции шифрования данных. Обеспечение безопасности файлов и папок. Аудит файлов. Шифрование файлов.
Раздел 5. Реализация системы безопасности сети в ОС MSWindows.
Утилиты по настройке сети. Угрозы сетевой безопасности, реализация брандмауэров. Настройка брандмауэра Windows. Защита доступа к сети. Установка дополнительной системы защиты информации, для упрощения управлением доступом к файлам, на примере системы SearchInform.

---

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

***Б1.В.16 Классификация и категорирование объектов, требующих особого порядка обеспечения информационной безопасности***

Цели освоения дисциплины

---

Целью преподавания дисциплины «Классификация и категорирование объектов, требующих особого порядка обеспечения информационной безопасности» является:
предоставить студентам навыками использования нормативных правовых актов, нормативных и методических документов ФСБ, ФСТЭК России в профессиональной деятельности; предоставить знания по выявлению критических процессов субъекта КИИ.

---

Место дисциплины в структуре ОП

---

Дисциплина «Классификация и категорирование объектов, требующих особого порядка обеспечения информационной безопасности» Б1.В.17 является дисциплиной части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки специалитета по направлению «10.05.02

Информационная безопасность телекоммуникационных систем». Изучение дисциплины «Классификация и категорирование объектов, требующих особого порядка обеспечения информационной безопасности» опирается на знании дисциплин(ы) «Защита информации в центрах обработки данных».

---

Требования к результатам освоения

---

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации; (ОПК-5)
– Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в процессе функционирования сетей электросвязи в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю; (ОПК-6)

---

Содержание дисциплины

---

Раздел 1. Телекоммуникации и их регулирование в правовой системе РФ.
Система норм права, регулирующих деятельность телекоммуникаций в РФ. Субординация норм права. Коллизии права. Конституционные основы деятельности в телекоммуникациях РФ.
Раздел 2. Правовые основы деятельности связи в РФ.
Федеральная связь РФ и ее состав. Сеть связи общего пользования. Выделенные сети связи. Технологические сети связи. Сети связи специального назначения. Государственное регулирование деятельности в области связи. Обязанности операторов связи в соответствии с федеральным законом РФ "О связи". Универсальные услуги связи.
Раздел 3. Информация, информационные технологии и защита информации в правовой системе РФ
Информация, информационные технологии, доступ к информации, предоставление информации, распространение информации в соответствии с законом РФ "Об информации, информационных технологиях и о защите информации". Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации в РФ.
Раздел 4. Государственная тайна в РФ.
Перечень сведений, составляющих государственную тайну в РФ. Сведения, не подлежащие отнесению к государственной тайне и засекречеванию в РФ. Допуск должностных лиц и граждан к государственной тайне. Особый порядок допуска к государственной тайне. Основания для отказа должностному лицу или гражданину в допуске к государственной тайне.
Раздел 5. Правовая защита персональных данных в РФ.
Персональные данные, их обработка, распространение, предоставление, блокирование, уничтожение и обезличивание в соответствии с федеральным законом РФ "О персональных данных". Принципы обработки персональных данных. Согласие субъекта персональных данных на обработку его персональных данных.

Раздел 6. Правовое регулирование в РФ информации, причиняющей вред здоровью и (или) развитию детей
Виды информации, причиняющей вред здоровью и (или) развитию детей. Классификация информационной продукции в соответствии с федеральным законом РФ "О защите детей от информации, причиняющих вред их здоровья и развитию".

---

Общая трудоемкость дисциплины

216 час(ов), 6 ЗЕТ

Форма промежуточной аттестации

Экзамен

### *Б1.В.17 Защита Web-приложений*

Цели освоения дисциплины

---

Целью преподавания дисциплины «Защита Web-приложений» является: ознакомление студентов с основными принципами проектирования Webприложений с использованием современных методик создания софтверной архитектуры.

---

Место дисциплины в структуре ОП

---

Дисциплина «Защита Web-приложений» Б1.В.17 является дисциплиной части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Изучение дисциплины «Защита Web-приложений» опирается на знании дисциплин(ы) «Автоматизация и модернизация операционных систем сетевых устройств»; «Компьютерные вирусы».

---

Требования к результатам освоения

---

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен использовать программные, программно-аппаратные и технические средства защиты информации при решении задач профессиональной деятельности; (ОПК-9)
– Способен устанавливать и настраивать антивирусные средства защиты информации в операционных системах (ПК-4)

---

Содержание дисциплины

Раздел 1. Определение архитектуры Web-приложений
Процесс разработки приложения. Анализ прецедентов. Архитектурные шаблоны Webприложений. Шаблон Thin Web Client. Шаблон Thick Web Client. Шаблон Web Delivery
Раздел 2. Требования и прецеденты при разработке Web-приложений
Требования. Формулировка требований. Рекомендации по написанию требований. Ранжирование. Прецеденты. Модель прецедентов. Диаграммы последовательностей. Анализ прецедентов
Раздел 3. Стадия анализа при разработке Web-приложений
Итеративность. Пакеты. Определение модели верхнего уровня. Анализ. Диаграммы последовательностей. Диаграммы сотрудничества. Диаграммы видов деятельности.
Раздел 4. Стадия проектирования при разработке Web-приложений
Расширение языка UML для Webприложений. Проектирование на основе шаблонов Thin Web Client, Thick Web Client, Web Delivery. Рекомендации по проектированию Web-приложений.
Раздел 5. Артефакты моделирования
Построение диаграмм путей в сайте. Составление тематической схемы. Интерактивная раскадровка. Функциональная спецификация. Инвентарная опись контента. Схема сайта. Разновидности схем. Словарь схемы сайта. Логическая схема сайта.

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

### *Б1.В.18 Сертификация средств защиты информации*

Цели освоения дисциплины

Целью преподавания дисциплины «Сертификация средств защиты информации» является:

предоставить студентам знания в области оценки соответствия средств защиты информации требованиям технических регламентов, положениям стандартов, сводов правил или условиям договоров, а также в области единой системы сертификации средств защиты информации (СЗИ) и аттестации объектов информатизации требованиям по безопасности информации, организация которой осуществляется ФСТЭК России.

Место дисциплины в структуре ОП

Дисциплина «Сертификация средств защиты информации» Б1.В.19 является дисциплиной части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки специалитета по направлению «10.05.02

Информационная безопасность телекоммуникационных систем». Изучение дисциплины «Сертификация средств защиты информации» опирается на знании дисциплин(ы) «Защита в операционных системах».

---

Требования к результатам освоения

---

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен оценивать технические возможности, анализировать угрозы и вырабатывать рекомендации по построению элементов информационно-телекоммуникационной инфраструктуры с учетом обеспечения требований информационной безопасности; (ОПК-13)
– Способен управлять проектом на всех этапах его жизненного цикла (УК-2)

---

Содержание дисциплины

---

Раздел 1. Сертификация средств защиты информации.
Законодательные, нормативные правовые акты, стандарты и методические документы, регламентирующие проведение работ по оценке соответствия требованиям по безопасности информации продукции. Организационная структура Системы сертификации ФСТЭК России.
Раздел 2. Программа и методика испытаний.
Порядок проведения сертификационных испытаний в Системе сертификации ФСТЭК России. Этапы, шаги, процедуры. Документальная проверка, инструментальный контроль, контроль выполнения процедур по безопасной разработке средств защиты информации.
Раздел 3. Подготовка к проведению сертификационных испытаний.
Предварительное ознакомление с изделием. Требования к разработке программ и методик сертификационных испытаний. Отбор образцов изделий.
Раздел 4. Профили защиты. Задание по безопасности.
Требования к разработке профилей защиты и заданий по безопасности.
Раздел 5. Испытания на соответствие ТУ.
Порядок проведения испытаний на соответствие техническим условиям.
Раздел 6. Методы выявления уязвимостей и НДВ.
Экспертный, статический, динамический, комбинированный и ручной анализы.
Раздел 7. Оформление отчетных материалов по результатам проведения сертификационных испытаний.
Требования по разработке отчетных материалов по результатам сертификационных испытаний. Содержание протоколов, заключений.
Раздел 8. Экспертиза материалов сертификационных испытаний.
Особенности проведения экспертизы материалов сертификационных испытаний средств защиты информации.
Раздел 9. Аттестация объектов информатизации.
Нормативное правовое обеспечение деятельности по аттестации объектов информатизации. Порядок проведения аттестации автоматизированных систем.
Раздел 10. Порядок проведения аттестационных испытаний.
Предварительное обследование объекта информатизации. Требования к разработке

программ и методик аттестационных испытаний. Документальная проверка и инструментальных контроль объектов информатизации. Порядок и требования к оформлению отчетных материалов по результатам аттестационных испытаний. Протоколы, заключения по результатам аттестационных испытаний.

---

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

### *Б1.В.19 Технологии обеспечения информационной безопасности больших данных*

Цели освоения дисциплины

---

Целью преподавания дисциплины «Технологии обеспечения информационной безопасности больших данных» является:

дать студентам знания о методах обработки больших данных, системах кластерных вычислений, неструктурированных базах данных и методах машинного обучения.

---

Место дисциплины в структуре ОП

---

Дисциплина «Технологии обеспечения информационной безопасности больших данных» Б1.В.20 является дисциплиной части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Изучение дисциплины «Технологии обеспечения информационной безопасности больших данных» опирается на знании дисциплин(ы) «Администрирование средств защиты информации в компьютерных системах и сетях»; «Защита в операционных системах»; «Защита информации в центрах обработки данных»; «Основы информационной безопасности»; «Основы проектирования защищенных инфокоммуникационных систем».

---

Требования к результатам освоения

---

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен применять методы научных исследований при проведении разработок в области функционирования, развития и обеспечения информационной безопасности телекоммуникационных систем и сетей; (ОПК-8)

Содержание дисциплины

Раздел 1. Hadoop.
Понятие больших данных. Экосистема Hadoop. Методы хранения и обработки неструктурированных и слабоструктурированных данных. Модель распределённых вычислений Map Reduce.
Раздел 2. Модель данных Yarn и инфраструктура кластерных вычислений Spark.
Apache Spark. Модуль, отвечающий за управление ресурсами кластеров и планирование заданий Yarn.
Раздел 3. Базы данных SQL и NoSQL.
Виды баз данных: от SQL, к NoSQL. Отличия.
Раздел 4. Архитектуры обработки Больших данных
Лямбда и Каппа архитектуры для обработки Больших данных, обзор, преимущества и недостатки решений, типовые решения.
Раздел 5. Системы контейнеризации.
Платформы для разработки, доставки и запуска контейнерных приложений. Основные инструменты и принципы контейнеризации.
Раздел 6. Методы машинного обучения
Обучение с учителем. Обучение без учителя. Глубокое обучение. Модели машинного обучения:DT, SVM.

Общая трудоемкость дисциплины

180 час(ов), 5 ЗЕТ

Форма промежуточной аттестации

Экзамен

### *Б1.В.20 Вредоносное программное обеспечение*

Цели освоения дисциплины

Целью преподавания дисциплины «Вредоносное программное обеспечение» является:

формирование у студентов профессиональных компетенций, связанных с использованием теоретических и практических знаний в области обеспечения информационной безопасности при проектировании, внедрении и эксплуатации информационных систем, а так же изучение структуры и принципов функционирования вредоносного программного обеспечения.

Место дисциплины в структуре ОП

Дисциплина «Вредоносное программное обеспечение» Б1.В.21 является дисциплиной части, формируемой участниками образовательных отношений блока

1 учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Изучение дисциплины «Вредоносное программное обеспечение» опирается на знании дисциплин(ы) «Ассемблер в задачах защиты информации»; «Компьютерные вирусы».

---

Требования к результатам освоения

---

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен создавать программы на языке высокого уровня, применять существующие реализации структур данных и алгоритмов; (ОПК-7)
– Способен конфигурировать и контролировать корректность настройки программно-аппаратных средств защиты информации в компьютерных сетях (ПК-8)
– Способен формулировать и обосновывать правила безопасной эксплуатации программного обеспечения (ПК-10)

---

Содержание дисциплины

---

Раздел 1. Компьютерные угрозы, основная классификация вредоносного ПО
Эволюция программ с вредоносным ПО, примеры
Раздел 2. Технологии атак, архитектура x86
Технологии атак, архитектура x86
Раздел 3. Фишинговые атаки, угрозы онлайн банкинга
Определение и классификация фишинговых атак, детекция атак, обзор угроз онлайн банкинга, примеры атак, методы защиты
Раздел 4. Программное обеспечение, предназначенное для вымогательства
Классификация угроз Ransom ware and Scareware. Примеры атак, методы защиты от угроз.
Раздел 5. Ботнеты
Определение, топологии, протоколы взаимодействия, примеры.
Раздел 6. Угрозы мобильных платформ: IOS
Классификация основных видов угроз IOS. Вирусы и уязвимости AppleIOS. Средства защиты.
Раздел 7. Угрозы мобильных платформ: Android
Обзор архитектуры Android. Примеры программ. Патчи, эксплоиты.
Раздел 8. Веб-угрозы, социальная инженерия, угрозы и уязвимости
Понятие уязвимостей и угроз. Web-эксплоиты, PDF, MSOffice, другие.
Раздел 9. Руткиты и буткиты
ОбзорWindows Kernel (ядра ОС Windows), понятие руткитов, эволюция руткитов. Понятие буткитов, эволюция.
Раздел 10. Антивирусные технологии
Определение комплексных антивирусов, классификация, современные антивирусные технологии
Раздел 11. Технологии sandbox
Определение sandbox. Доступные решения на рынке для борьбы с вредоносным ПО

Раздел 12. Определение вредоносного ПО, интеллектуальный анализ данных
Основные средства борьбы с вредоносным ПО, интеллектуальный анализ данных

---

Общая трудоемкость дисциплины

252 час(ов), 7 ЗЕТ

Форма промежуточной аттестации

Экзамен. Курсовая работа

### *Б1.В.21 Цифровая криминалистика*

Цели освоения дисциплины

---

Целью преподавания дисциплины «Цифровая криминалистика» является: формирование фундамента подготовки будущих специалистов в области цифровых доказательств, а также, создавать необходимую базу для успешного овладения последующими специальными дисциплинами учебного плана. Она должна способствовать развитию творческих способностей студентов, умению формулировать и решать задачи изучаемой специальности, умению творчески применять и самостоятельно повышать свои знания.

---

Место дисциплины в структуре ОП

---

Дисциплина «Цифровая криминалистика» Б1.В.22 является дисциплиной части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Изучение дисциплины «Цифровая криминалистика» опирается на знании дисциплин(ы) «Защита в операционных системах».

---

Требования к результатам освоения

---

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен проводить инструментальный мониторинг качества обслуживания и анализ защищенности информации от несанкционированного доступа в телекоммуникационных системах и сетях в целях управления их функционированием; (ОПК-15)
– Способен анализировать угрозы безопасности информации программного обеспечения (ПК-9)

---

Содержание дисциплины

Раздел 1. Введение в цифровые доказательства
Значение термина цифровой форензики, стандартные процедуры, методы написания отчетов, технологии документирования, стандарты для идентификации, сбора информации (ISO/IEC 27037), описание инструментов с кратким анализом функционала xmount, guymager, ewf-tools, и т.д., настройка рабочей станции.
Раздел 2. Работа с данными
Создание образа для цифровой форензики: описание инструментария, команды Linux, форматы образов (dd, ewf), хеширование (контроль за целостностью данных – функции MD5, SHA1, SHA256).
Раздел 3. Работа с жесткими дисками
Физические и логические тома, функции: образы для разбиения дисков, MBR, GPT, обзор функций RAID-массивов.
Раздел 4. Файловые системы
FAT, основные функции NTFS, основные функции HFS and HFS+.
Раздел 5. Анализ работы операционных систем на примере семейства ОС Windows
Анализ логов ОС Windows, конфигурационного регистра, браузеров, метаданных.
Раздел 6. Анализ интернет приложений ОС Windows
Браузеры, мессенджеры, p2p приложения, инструментарии для анализа приложений Windows (sqllite-bowser), шифрование (bitlockers).
Раздел 7. Анализ уязвимостей ОС Linux, MacOS
Анализ логов, истории активности пользователей, конфигурация.
Раздел 8. Анализ уязвимостей MacOS
Анализ логов, истории активности пользователей, конфигурация.
Раздел 9. Сетевая форензика
Перехват сетевого трафика, анализ уровня приложений, инструментарий для сетевой форензики (Wireshark, Ettercap, другие).
Раздел 10. Форензика в реальном времени
Обслуживание машин в реальном времени, функции данных в реальном времени на примере ОС Windows, Linux, Mac OS).
Раздел 11. Форензика SSD
Инструментарии для работы с форензикой SSD, функциональные особенности.
Раздел 12. Форензика памяти
Основы работы с анализом памяти, аналитика дампов памяти RAM.

---

Общая трудоемкость дисциплины

252 час(ов), 7 ЗЕТ

Форма промежуточной аттестации

Экзамен. Курсовая работа

### *Б1.В.22 Межсетевое экранирование и системы предотвращения вторжений*

Цели освоения дисциплины

---

Целью преподавания дисциплины «Межсетевое экранирование и системы

предотвращения вторжений» является:
дать слушателям знания по внедрению системы предотвращения вторжений следующего поколения, а также о межсетевых экранах нового поколения.

---

Место дисциплины в структуре ОП

---

Дисциплина «Межсетевое экранирование и системы предотвращения вторжений» Б1.В.23 является дисциплиной части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Изучение дисциплины «Межсетевое экранирование и системы предотвращения вторжений» опирается на знании дисциплин(ы) «Введение в профессию»; «Защита операционных систем сетевых устройств»; «Основы информационной безопасности»; «Основы маршрутизации в компьютерных сетях»; «Основы построения защищенных компьютерных сетей»; «Принципы организации глобальных вычислительных сетей»; «Сети и системы передачи информации».

---

Требования к результатам освоения

---

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в процессе функционирования сетей электросвязи в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю; (ОПК-6)
– Способен настраивать правила фильтрации пакетов в компьютерных сетях (ПК-7)

---

Содержание дисциплины

---

Раздел 1. Введение в специализированные устройства безопасности.
Введение в специализированные устройства безопасности на примере Cisco ASA, описание линейки Cisco ASA.
Раздел 2. Внедрение базовых функций межсетевого экрана по обеспечению связи и управлению устройством.
Работа с Cisco ASA и графическим средством управления ASDM. Настройка интерфейсов и статической маршрутизации. Настройка базовых функций по управлению устройством.
Раздел 3. Внедрение функций по контролю доступа.
Настройка функций NAT на устройстве Cisco ASA. Настройка базового контроля доступа. Тонкая настройка базовых функций инспектирования, основанного на состоянии сессии. Настройка продвинутых функций контроля доступа.
Раздел 4. Обзор VPN-компонентов для Cisco ASA

Обзор технологий VPN. Реализация профилей, групповых политик и пользовательских политик. Внедрение сервисов PKI. Внедрение Clientless SSL VPN
Раздел 5. Выполнять первоначальную настройку сенсора IPS
Принципы работы сенсоров. Сигнатуры, настройка сигнатур, ложное срабатывание.
Раздел 6. IPS Cisco FirePOWER следующего поколения
Описание системы Cisco FireSIGHT. Настройка и управление устройствами Cisco FirePOWER. Внедрение политики контроля доступа. Понимание технологии обнаружения устройств и объектов в сети. Настройка обнаружения файлов и сетевых вредоносных программ.

---

Общая трудоемкость дисциплины

180 час(ов), 5 ЗЕТ

Форма промежуточной аттестации

Экзамен

### *Б1.В.23 Системы мониторинга безопасности защищенного объекта информатизации*

Цели освоения дисциплины

---

Целью преподавания дисциплины «Системы мониторинга безопасности защищенного объекта информатизации» является:
предоставить студентам навыками использования нормативных правовых актов, нормативных и методических документов ФСБ, ФСТЭК России в профессиональной деятельности; предоставить знания по выявлению критических процессов субъекта КИИ.

---

Место дисциплины в структуре ОП

---

Дисциплина «Системы мониторинга безопасности защищенного объекта информатизации» Б1.В.23 является дисциплиной части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Изучение дисциплины «Системы мониторинга безопасности защищенного объекта информатизации» опирается на знании дисциплин(ы) «Комплексная защита объектов информатизации»; «Основы информационной безопасности»; «Основы проектирования систем защиты объектов информатизации».

---

Требования к результатам освоения

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен применять методы научных исследований при проведении разработок в области функционирования, развития и обеспечения информационной безопасности телекоммуникационных систем и сетей; (ОПК-8)
– Способен формулировать и настраивать политики безопасности операционных систем (ПК-1)
– Способен устанавливать и настраивать антивирусные средства защиты информации в операционных системах (ПК-4)
– Способен проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах (ПК-5)
– Способен конфигурировать и контролировать корректность настройки программно-аппаратных средств защиты информации в компьютерных сетях (ПК-8)

---

Содержание дисциплины

---

Раздел 1. Телекоммуникации и их регулирование в правовой системе РФ.
Система норм права, регулирующих деятельность телекоммуникаций в РФ. Субординация норм права. Коллизии права. Конституционные основы деятельности в телекоммуникациях РФ.
Раздел 2. Правовые основы деятельности связи в РФ.
Федеральная связь РФ и ее состав. Сеть связи общего пользования. Выделенные сети связи. Технологические сети связи. Сети связи специального назначения.
Государственное регулирование деятельности в области связи. Обязанности операторов связи в соответствии с федеральным законом РФ "О связи". Универсальные услуги связи.
Раздел 3. Информация, информационные технологии и защита информации в правовой системе РФ
Информация, информационные технологии, доступ к информации, предоставление информации, распространение информации в соответствии с законом РФ "Об информации, информационных технологиях и о защите информации". Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации в РФ.
Раздел 4. Государственная тайна в РФ.
Перечень сведений, составляющих государственную тайну в РФ. Сведения, не подлежащие отнесению к государственной тайне и засекречиванию в РФ. Допуск должностных лиц и граждан к государственной тайне. Особый порядок допуска к государственной тайне. Основания для отказа должностному лицу или гражданину в допуске к государственной тайне.
Раздел 5. Правовая защита персональных данных в РФ.
Персональные данные, их обработка, распространение, предоставление, блокирование, уничтожение и обезличивание в соответствии с федеральным законом РФ "О персональных данных". Принципы обработки персональных данных. Согласие субъекта персональных данных на обработку его персональных данных.
Раздел 6. Правовое регулирование в РФ информации, причиняющей вред здоровью и (или) развитию детей
Виды информации, причиняющей вред здоровью и (или) развитию детей. Классификация информационной продукции в соответствии с федеральным законом РФ "О защите детей

от информации, причиняющих вред их здоровья и развитию".

---

Общая трудоемкость дисциплины

252 час(ов), 7 ЗЕТ

Форма промежуточной аттестации

Экзамен

***Б1.В.24 Тестирование на проникновение и этичный хакинг***

Цели освоения дисциплины

---

Целью преподавания дисциплины «Тестирование на проникновение и этичный хакинг» является:

получение знаний и навыков, необходимых для успешного выявления и устранения проблем безопасности в смешанных компьютерных сетях.

---

Место дисциплины в структуре ОП

---

Дисциплина «Тестирование на проникновение и этичный хакинг» Б1.В.25 является дисциплиной части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Изучение дисциплины «Тестирование на проникновение и этичный хакинг» опирается на знании дисциплин(ы) «Защита информации в центрах обработки данных».

---

Требования к результатам освоения

---

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен проводить инструментальный мониторинг качества обслуживания и анализ защищенности информации от несанкционированного доступа в телекоммуникационных системах и сетях в целях управления их функционированием; (ОПК-15)
– Способен оценивать угрозы безопасности информации операционных систем (ПК-2)
– Способен конфигурировать и контролировать корректность настройки программно-аппаратных средств защиты информации в компьютерных сетях (ПК-8)

---

Содержание дисциплины

---

Раздел 1. Сканирование и рекогносцировка в сетевой IP-инфраструктуре

Основные методы идентификации устройств в IP-сети, программное обеспечение для проведения идентификации. Сканирование сетевой инфраструктуры и определение топологии сети

Раздел 2. Эксплуатация уязвимостей операционных и SCADAсистем

Основные методы поиска уязвимостей операционных систем (Windows, Linux, MacOS). Методы эксплуатации уязвимостей. Использование п/о rootkits, keylogger. Эксплуатация уязвимостей файловых систем и подсистем ввода/вывода информации. Основы поиска уязвимостей SCADA-систем

Раздел 3. Перехват трафика

Основные методы перехвата трафика на канальном и сетевом уровне, в соответствии со стеком протоколов TCP/IP. Эксплуатация уязвимостей типа подмены MAC, IP-адресов. Атаки на ARPпротокол. Основное п/о для эксплуатации уязвимостей такого типа.

Раздел 4. Отказы в обслуживании

Проведение атак типа «Отказ в обслуживании» и «Распределенный отказ в обслуживании». Основное п/о для проведения атак такого типа. Принципы атак такого типа.

Раздел 5. Перехват сессийи сетевых соединений

Основные методы поиска уязвимостей в реализации протоколов сетевого и транспортного уровней, в соответствии со стеком протоколов TCP/IP. Методы эксплуатации уязвимостей такого типа. Перехват соединений TCP. Основное п/о для эксплуатации уязвимостей такого типа.

Раздел 6. Эксплуатация уязвимостей WEB-сервисов и приложений

Основные методы поиска и эксплуатации уязвимостей WEB-сервисов (HTTP)и WEB-приложений (с использование языков программирования Java, PHP). Исследование SQL-инъекций.

Раздел 7. Поиск и эксплуатация уязвимостей беспроводных сетей, работающих по стандарту 802.11

Основные методы поиска и эксплуатации уязвимостей беспроводных сетей Wi-Fi. Основные уязвимости в протоколах безопасности WEP, WPA/WPA2. П/о для эксплуатации уязвимостей такого типа.

Раздел 8. Поиск уязвимостей в мобильных устройствах

Основные методы поиска и эксплуатации уязвимостей в мобильных устройствах, в том числе эксплуатация уязвимостей персональных беспроводных сетей Bluetooth, ZigBee.

Раздел 9. Методы обхода систем предотвращения вторжений и межсетевых экранов

Основные методы поиска и эксплуатации уязвимостей в работе систем предотвращения вторжений и межсетевых экранов. Программное обеспечение, позволяющее эксплуатировать уязвимости такого типа

Раздел 10. Использование вирусов, закладок в коде. Переполнение буффера

Основные методы использования вредоносного п/о при проведении анализа уязвимостей инфокоммуникационных систем. Использование ошибок в программном коде для проведения атак типа «Переполнение буффера».

Раздел 11. Поиск уязвимостей в реализациях криптографических алгоритмов

Основные методы эксплуатации уязвимостей реализованных криптографических алгоритмов для проведения атак на виртуальные частные сети.

Раздел 12. Методы сокрытия деятельности в сети.

Основные методы анонимизации присутствия в цифровом пространстве и методы сокрытия деятельности, связанной с сетевой активностью

---

Общая трудоемкость дисциплины

252 час(ов), 7 ЗЕТ

Форма промежуточной аттестации

Экзамен

***Б1.В.25 Построение доверенной среды передачи***

Цели освоения дисциплины

Целью преподавания дисциплины «Построение доверенной среды передачи» является:

предоставить студентам знания о методах построения виртуальных частных сетей с использованием отечественного оборудования на примере централизованного комплекса для защиты сетевой инфраструктуры и создания VPN-сетей с использованием алгоритмов ГОСТ.

Место дисциплины в структуре ОП

Дисциплина «Построение доверенной среды передачи» Б1.В.26 является дисциплиной части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Изучение дисциплины «Построение доверенной среды передачи» опирается на знании дисциплин(ы) «Защита multicast трафика в сети Интернет»; «Защита в операционных системах»; «Основы информационной безопасности»; «Основы маршрутизации в компьютерных сетях»; «Основы построения защищенных компьютерных сетей»; «Основы проектирования защищенных инфокоммуникационных систем»; «Сети и системы передачи информации».

Требования к результатам освоения

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

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

– Способен проектировать защищенные телекоммуникационные системы и их элементы, проводить анализ проектных решений по обеспечению заданного уровня безопасности и требуемого качества обслуживания телекоммуникационных систем, разрабатывать необходимую техническую документацию с учетом действующих нормативных и методических документов, проводить подготовку исходных данных для технико-экономического обоснования соответствующих проектных решений; (ОПК-16)
– Способен оценивать угрозы безопасности информации в компьютерных сетях (ПК-6)

---

Содержание дисциплины

---

Раздел 1. Общие сведения по Континент.
Назначение и состав комплекса. Принципы функционирования комплекса. Управление комплексом. Типовые аппаратные платформы и их производительность. Порядок ввода комплекса в эксплуатацию.
Раздел 2. Управление узлами Континент.
Роли администраторов. Назначение администраторов. Дистанционный доступ по протоколу SSH.
Раздел 3. Настройка межсетевого экранирования.
Обработка трафика узлом безопасности. Межсетевое экранирование. Сетевые функции. Виды объектов ЦУС. Правила фильтрации.
Раздел 4. Детектор атак.
Концепция управления СОВ. Управление детектором атак в режимах Monitor и Inline. Установка БРП. Создание собственных сигнатур.
Раздел 5. Построение VPN.
VPN-туннель. Шифрование. VPN с аппаратным ускорением шифрования. L2VPN-туннель. VPN удаленного доступа.
Раздел 6. Обеспечение отказоустойчивости комплекса.
Резервирование и восстановление конфигурации. Аппаратное резервирование и восстановление УБ. Резервирование БД ЦУС.
Раздел 7. Мониторинг и аудит.
Общие сведения по системе мониторинга: инициализация, объекты мониторинга и типы информации, применение правил и шаблонов. Просмотр сведений журналов. Аудит.

---

Общая трудоемкость дисциплины

216 час(ов), 6 ЗЕТ

Форма промежуточной аттестации

Экзамен

### *Б1.В.ДВ.01.01 Безопасность беспроводных локальных сетей*

Цели освоения дисциплины

---

Целью преподавания дисциплины «Безопасность беспроводных локальных сетей» является:
приобретение студентами теоретических знаний по формализации структуры

и формированию соответствующих моделей для описания и анализа структуры, состава, алгоритмов работы беспроводных сетей.

---

Место дисциплины в структуре ОП

---

Дисциплина «Безопасность беспроводных локальных сетей» Б1.В.ДВ.01.01 является дисциплиной по выбору части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Защита информации с помощью маршрутизаторов и коммутаторов»; «Информатика»; «Основы информационной безопасности»; «Сети и системы передачи информации».

---

Требования к результатам освоения

---

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности; (ОПК-2)
– Способен настраивать правила фильтрации пакетов в компьютерных сетях (ПК-7)
– Способен конфигурировать и контролировать корректность настройки программно-аппаратных средств защиты информации в компьютерных сетях (ПК-8)

---

Содержание дисциплины

---

Раздел 1. Введение в беспроводные сети стандарта семейства IEEE 802.11
IEEE 802.11 — набор стандартов связи для коммуникации в беспроводной локальной сетевой зоне частотных диапазонов 2,4 и 5 ГГц.
Раздел 2. Основные принципы радиоанализа и радиопланирования
Принципы распределения радиоволн, виды антенн, принципы планирования беспроводной локальной, расчет допустимой мощности.
Раздел 3. Классификация элементов беспроводной локальной сети и организация сети семейства IEEE 802.11 на основе контроллера WLAN
Классификация элементов беспроводной локальной сети. Назначение контроллеров беспроводных сетей и их функционал. Принцип настройки.
Раздел 4. Основы и принципы работы протокола RADIUS, семейство протоколов EAP
Протоколы RADIUS, семейство протоколов EAP EAP и их применение в защищенных беспроводных сетях.
Раздел 5. Стандарт IEEE 802.1x, технологии профилирования и динамического изменения авторизации в беспроводных сетях семейства IEEE 802.11
IEEE 802.1x – стандарт аутентификации пользователей в сети. Применение IEEEE 802.1x

и технологий профилирования для обеспечения информационной безопасности беспроводных сетей. Технология динамического изменения авторизации.
Раздел 6. Технологии организации доступа в беспроводных сетях семейства IEEE 802.11
Описание принципов доступа беспроводных клиентов к сетям IEEE 802.11. Структура кадра IEEE 802.11.
Раздел 7. Протоколы и механизмы информационной безопасности в беспроводных сетях семейства IEEE 802.11
Классификация механизмов информационной безопасности беспроводных сетей. Протоколы информационной безопасности согласно стандарту IEEE 802.11 . Дополнительные механизмы повышения уровня защищенности беспроводной сети.

---

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет. Курсовая работа

***Б1.В.ДВ.01.02 Защищенные мобильные приложения***

Цели освоения дисциплины

---

Целью преподавания дисциплины «Защищенные мобильные приложения» является:
является получение знаний и навыков разработки защищенных мобильных приложений

---

Место дисциплины в структуре ОП

---

Дисциплина «Защищенные мобильные приложения» Б1.В.ДВ.01.02 является дисциплиной по выбору части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Основы информационной безопасности»; «Разработка защищенных сетевых приложений».

---

Требования к результатам освоения

---

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности; (ОПК-2)
– Способен настраивать правила фильтрации пакетов в компьютерных сетях (ПК-7)
– Способен конфигурировать и контролировать корректность настройки программно-аппаратных средств защиты информации в компьютерных сетях (ПК-8)

---

Содержание дисциплины

---

Раздел 1. Классификация мобильных устройств и мобильных операционных систем
Мини- микрокомпьютеры, операционные системы, применяемые в мобильных устройствах и их сравнение.
Раздел 2. Инструментарий разработки мобильных приложений
Знакомство с инструментарием разработки мобильных приложений на примере Android studio. Версионирование мобильных приложений.
Раздел 3. Эмуляторы мобильных устройства
Обзор эмуляторов мобильных устройств. Особенности использования BlueStacks, а также развертывание Android ОС на базе продуктов VMWare.
Раздел 4. Структура и компоненты Android приложений
Изучение структуры и компонентов Android приложений. Знакомство с Fragments. Изучение IntentExtras для реализации многоэкранных мобильных приложений. Знакомство с Play Market.
Раздел 5. Хранение данных в мобильных приложения
Изучение подходов хранения данных в мобильных приложениях. Особенности работы с файлами на ОС Android.
Раздел 6. Работа с базами данных
Классификация баз данных, применяемых в мобильных приложениях. Основы языка SQL. Особенности работы со встроенной базой данный SQLite.
Раздел 7. Работа с webсервисами в мобильных приложениях
Краткое описание web-сервисов и их применение в мобильных приложениях. Развертывание Webсервиса для мобильных устройств.
Раздел 8. Обзор механизмов безопасности, применяемых в мобильной операционной системе Android
Основные механизмы информационной безопасности в ОС Android и их эволюция.
Раздел 9. Коммуникационные технологии WWAN для мобильных устройств
Стандарт группы 3G/4G/5G и основы организации беспроводной сети на базе этих стандартов.
Раздел 10. Коммуникационные технологии WLAN для мобильных устройств
Стандарты семейства IEEE 802.11 и их использование в современных мобильных устройствах.

---

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет. Курсовая работа

***Б1.В.ДВ.02.01 Безопасность IP-телефонии***

Цели освоения дисциплины

Целью преподавания дисциплины «Безопасность IP-телефонии» является: изучение архитектуры, настройки IP-телефонии. Формирование у студентов компетентности в области средств и систем передачи голоса и видео при помощи сетей связи (IP-телефонии).

Место дисциплины в структуре ОП

Дисциплина «Безопасность IP-телефонии» Б1.В.ДВ.02.01 является дисциплиной по выбору части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Аппаратные средства вычислительной техники»; «Безопасность Astra-Linux»; «Безопасность беспроводных локальных сетей»; «Введение в профессию»; «Защита в операционных системах»; «Защита программ и данных».

Требования к результатам освоения

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности; (ОПК-2)
– Способен проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах (ПК-5)
– Способен оценивать угрозы безопасности информации в компьютерных сетях (ПК-6)

Содержание дисциплины

Раздел 1. Введение в VoIP.
Определение IP-телефонии. История. Конвергенция сетей связи. Понятие АТС, протоколы IPтелефонии. Оборудование . Стандартизация IPтелефонии. Правовое регулирование IP-телефонии в России.
Раздел 2. Автоматические телефонные станции (АТС).
Виды АТС. Вендоры. Функции АТС.
Раздел 3. Elastix PBX.
Конфигурирование Elastix. Функции Elastix. Подключение дополнительного оборудования к Elastix. Настройка телефонов.
Раздел 4. АТС Агат UX.

Конфигурирование Агат UX. Функции Агат UX. Подключение дополнительного оборудования к Агат UX. Настройка телефонов.
Раздел 5. Cisco CUCM.
Конфигурирование Cisco CUCM. Функции Cisco CUCM. Подключение дополнительного оборудования к Cisco CUCM. Настройка телефонов.
Раздел 6. Безопасность VoiP ч 1.
Протоколы безопасности на модели OSI. Шифрование. Аутентификация.
Раздел 7. Безопасность VoiP ч 2.
Настройка защищенной телефонии на оборудование различных вендоров.
Раздел 8. Введение в QoS.
Обзор QoS. Задача QoS. Цели QoS. Оборудование поддерживающее QoS.
Раздел 9. Изучение характеристик трафика.
Задержка . Потеря пакетов. Джиттер .
Раздел 10. Управление трафиком с помощью технологии QoS.
Настройка QoS на оборудовании Cisco. Class map. Policy map.

---

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

### *Б1.В.ДВ.02.02 Защита multicast трафика в сети Интернет*

Цели освоения дисциплины

---

Целью преподавания дисциплины «Защита multicast трафика в сети Интернет» является:

осветить базовые понятия и особенности работы технологии IP Multicast. Под ними подразумеваются: приложения, использующие многоадресной рассылку, источники рассылки, получатели рассылки, управление группами рассылки, протоколы маршрутизации трафика (например, Protocol Independent Multicast, PIM) и их работа внутри одного административного домена. В рамках дисциплины рассмотрены способы обеспечения надежности работы технологии многоадресной рассылки. Описаны варианты внедрения технологии в корпоративной сети и в сети провайдера услуг. В рамках программы рассматриваются способы настройки IP Multicast на маршрутизаторах.

---

Место дисциплины в структуре ОП

---

Дисциплина «Защита multicast трафика в сети Интернет» Б1.В.ДВ.02.02 является дисциплиной по выбору части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем».

Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Введение в профессию»; «Защита операционных систем сетевых устройств»; «Основы информационной безопасности»; «Основы маршрутизации в компьютерных сетях»; «Сети и системы передачи информации».

---

Требования к результатам освоения

---

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности; (ОПК-2)
– Способен проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах (ПК-5)
– Способен оценивать угрозы безопасности информации в компьютерных сетях (ПК-6)

---

Содержание дисциплины

---

Раздел 1. Концепции и технологии, заложенные в основу IP Multicast.
Введение в IP Multicast. Понимание модели сервисов многоадресной рассылки. Объяснение деревьев распространения многоадресной рассылки. Рассмотрение протоколов для работы IP Multicast.
Раздел 2. Multicast в локальных сетях.
Перевод сетевых адресов в канальные. Рассмотрение работы протокола CGMP. Использование IGMP Snooping.
Раздел 3. Режим PIM Sparse Mode.
Введение в PIM-SM. Понимание механизмов протокола PIM-SM. Варианты использования протокола PIM в Sparse Mode. Настройка и мониторинг PIM-SM.
Раздел 4. Конфигурация точки распределения Rendezvous Point.
Рассмотрение вариантов распространения информации о RP. Описание и внедрение Auto-RP. Описание и внедрение PIMv2 BSR. Описание и внедрение Anycast RP и протокола MSDP.
Раздел 5. Расширения протокола PIM в режиме Sparse Mode.
Введение в Source Specific Multicast (SSM). Рассмотрение Bidirectional PIM.
Раздел 6. Мультипротокольные расширения для BGP.
Введение в MP-BGP. Настройка и мониторинг MPBGP.
Раздел 7. IP Multicast между доменами.
Рассмотрение динамического меж доменного IP multicast. Рассмотрение протокола Multicast Source Discovery Protocol (MSDP).
Раздел 8. Защита трафика IP Multicast.
Введение в безопасность в IP Multicast. Защита сетей многоадресной рассылки.

---

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

***Б1.В.ДВ.03.01 Блокчейн и обеспечение безопасности распределенных реестров***

Цели освоения дисциплины

Целью преподавания дисциплины «Блокчейн и обеспечение безопасности распределенных реестров» является:
изучение технологии блокчейн, криптографических основ построения распределенных реестров. Дисциплина "Блокчейн и обеспечение безопасности распределенных реестров" должна обеспечивать формирование фундамента подготовки будущих специалистов в области защиты данных и блокчейна, а также, создавать необходимую базу для успешного изучения методов защиты информации.

Место дисциплины в структуре ОП

Дисциплина «Блокчейн и обеспечение безопасности распределенных реестров» Б1.В.ДВ.03.01 является дисциплиной по выбору части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Криптографические протоколы»; «Методы и средства криптографической защиты информации».

Требования к результатам освоения

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен использовать методы и средства криптографической защиты информации при решении задач профессиональной деятельности; (ОПК-10)

Содержание дисциплины

Раздел 1. Введение в дисциплину.
Понятие распределенных реестров, централизованных и децентрализованных систем. Основы технологии блокчейн и сферы её применения. Связь криптографии и блокчейна.
Раздел 2. Криптографические преобразования в блокчейне. Методы шифрования и хеширования.

Функции хеширования. Свойства хеш-функций. Алгоритмы шифрования. Симметричные и асимметричные алгоритмы. Криптография на эллиптических кривых. Электронная цифровая подпись. Мультиподписи.
Раздел 3. Концепции криптологии, информатики и теории игр в блокчейне
Свойства решений основанных на блокчейне. Задача византийских генералов. Хэш-указатели. Дерево Меркла. Транзакции в блокчейн.
Раздел 4. Свойства блокчейна и распределенных реестров. Блокчейн приложения.
Механизмы распределенного консенсуса. Криптовалюты как блокчейн приложения. Архитектура платформ Bitcoin, Ethereum Механизмы функционирования Bitcoin. Ethereum Примеры использования.
Раздел 5. Разработка блокчейн-приложений.
Децентрализованные приложения. Создание блокчейн-приложений. Программирование приложений Bitcoin и Ethereum. Программное взаимодействие с блокчейном. Использование частных и тестовых блокчейнов. Создание и размещение смарт-контракта. Обращение к смарт-контракту.
Раздел 6. Области применения распределенных реестров.
Публичные и частные блокчейны. IoT и системы распределенного реестра. Решение прикладных задач на основе блокчейна. Перспективы технологии.

---

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

***Б1.В.ДВ.03.02 Основы криптографии с открытым ключом***

Цели освоения дисциплины

---

Целью преподавания дисциплины «Основы криптографии с открытым ключом» является:

является изучение вопросов основ криптографической защиты с открытым ключом информации в телекоммуникационных системах. Дисциплина «Основы криптографии с открытым ключом» должна обеспечивать формирование фундамента подготовки будущих бакалавров в области инфокоммуникаций, а также, создавать необходимую базу для успешного овладения последующими специальными дисциплинами учебного плана.

---

Место дисциплины в структуре ОП

---

Дисциплина «Основы криптографии с открытым ключом» Б1.В.ДВ.03.02 является дисциплиной по выбору части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем».

Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Блокчейн и эллиптическая криптография»; «Введение в профессию»; «Криптографические протоколы»; «Математический анализ»; «Методы и средства криптографической защиты информации».

---

Требования к результатам освоения

---

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен использовать методы и средства криптографической защиты информации при решении задач профессиональной деятельности; (ОПК-10)

---

Содержание дисциплины

---

Раздел 1. Основы построения криптосистем с открытым ключом
Введение в курс. Основные понятия и определения.
Раздел 2. Квадратичные вычеты. Генерирование простых чисел
Модульная арифметика,возведение в степень логарифмирование Конечные поля, способы представления. Оценки сложности вычислений. Квадратичные вычеты и тестирование простых чисел.
Раздел 3. Криптосистема РША и анализ ее стойкости
Криптосистема РША. Генерирование ключей, шифрование, дешифрование.
Раздел 4. Криптосистемы Рабина,Уильямса, Голдвассера-Микали, Эль-Гамаля и Диффи-Хеллмана
Криптосистемы Эль-Гамаля, Рабина. Генерирование ключей, шифрование, дешифрование.
Раздел 5. Квантовые вычисления и оценка стойкости криптоалгоритмов
Построение криптосистем на основе эллиптических кривых. Бесключевые хэш-функции. Модель электронной цифровой подписи сообщения, виды ЭЦП. ЭЦП на основе различных криптосистем. Стандарты ЭЦП и хэш-функции.
Раздел 6. Криптосистема Мак-Элис и анализ ее стойкости
Криптосистема Мак-Элис. Генерирование ключей, шифрование, дешифрование.
Раздел 7. Гомоморфное шифрование
Основные принципы взаимодействия с зашифрованными сообщениями.
Раздел 8. Криптографические протоколы (обзор)
Принцип построения инфраструктуры открытых ключей (PKI), назначение и использование сертификатов открытых ключей.
Раздел 9. Протоколы разделения секрета
Обзор основных протоколов. Изучение протоколов разделения секрета, аутентификация пользователей с нулевым разглашением, секретные совместные вычисления, тайное голосование.
Раздел 10. Протоколы распределения ключей
Распределение ключей для симметричных систем на основе криптографии с открытыми ключами.

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

***Б1.В.ДВ.04.01 Защита операционных систем сетевых устройств***

Цели освоения дисциплины

Целью преподавания дисциплины «Защита операционных систем сетевых устройств» является:

дать студентам представление о функциях сетевых устройств, об уязвимостях сетевых протоколов стека TCP/IP, об особенностях функционирования операционных систем конечных устройств. Студенты узнают о концепциях сетевой информационной безопасности, распространенных сетевых протоколах и их уязвимостях, об атаках на сетевые приложения и операционные системы Windows и Linux, научатся использовать полученные знания для расследования инцидентов безопасности в защищаемой инфраструктуре. После прохождения данного курса студенты будут обладать базовыми знаниями, необходимыми для выполнения работы аналитика кибербезопасности начального уровня в центре обеспечения безопасности, ориентированном на выявление угроз безопасности и повышение эффективности использования существующей инфраструктуры.

Место дисциплины в структуре ОП

Дисциплина «Защита операционных систем сетевых устройств» Б1.В.ДВ.04.01 является дисциплиной по выбору части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Введение в профессию»; «Основы информационной безопасности»; «Сети и системы передачи информации».

Требования к результатам освоения

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства; (ОПК-1)
– Способен оценивать угрозы безопасности информации операционных систем (ПК-2)
– Способен устанавливать и настраивать антивирусные средства защиты информации в операционных системах (ПК-4)
– Способен настраивать правила фильтрации пакетов в компьютерных сетях (ПК-7)

---

Содержание дисциплины

---

Раздел 1. Кибербезопасность и центр мониторинга и управления безопасностью.
Операционный центр безопасности (SOC). Технологии и процессы в SOC.
Раздел 2. Операционные системы.
Архитектура Windows, принципы работы политики безопасности, уязвимости. Администрирование Windows. Администрирование Linux. Контроль журналов служб.
Раздел 3. Сетевые протоколы и службы. Инфраструктура сети.
Основные протоколы и службы обеспечения функционирования компьютерной сетью: IP, ARP, DHCP, DNS, FTP, TFTP, TCP, UDP. Сетевые устройства связи, межсетевые экраны, маршрутизаторы, коммутаторы. Протокол NetFlow. Серверы AAA, зеркалирование портов.
Раздел 4. Принципы обеспечения сетевой безопасности.
Мониторинг сети и средства мониторинга. Атаки на базовые функции. Категории сетевых атак. Обнаружение угроз. Уязвимость и поверхность атаки. Эксплоит и риски. Описание подходов к защите сети. Контроль доступа. Аналитика угроз.
Раздел 5. Шифрование и инфраструктура открытых ключей.
Симметричные и асимметричные шифры. Алгоритмы хеш-функций. PKI.
Раздел 6. Защита и анализ оконечных устройств.
Защита оконечных устройств. Оценка уязвимостей оконечных устройств. CVSS отчеты.
Раздел 7. Мониторинг безопасности.
Технологии и протоколы. Файлы журналов. Описание типов файлов журналов, используемых в мониторинге безопасности. Оценка предупреждений. Работа с данными безопасности сети. Цифровая техническая экспертиза. Модели реагирования на инциденты. Обработка инцидентов.

---

Общая трудоемкость дисциплины

216 час(ов), 6 ЗЕТ

Форма промежуточной аттестации

Экзамен

### *Б1.В.ДВ.04.02 Защита информации с помощью маршрутизаторов и коммутаторов*

Цели освоения дисциплины

---

Целью преподавания дисциплины «Защита информации с помощью маршрутизаторов и коммутаторов» является:

дать студентам общее представление о механизмах защиты маршрутизаторов и коммутаторов в компьютерных сетях, рассмотреть методы построения виртуальных частных сетей, технологии трансляции сетевых адресов NAT/PAT.

---

Место дисциплины в структуре ОП

---

Дисциплина «Защита информации с помощью маршрутизаторов и коммутаторов» Б1.В.ДВ.04.02 является дисциплиной по выбору части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Основы информационной безопасности»; «Сети и системы передачи информации».

---

Требования к результатам освоения

---

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства; (ОПК-1)
– Способен оценивать угрозы безопасности информации операционных систем (ПК-2)
– Способен устанавливать и настраивать антивирусные средства защиты информации в операционных системах (ПК-4)
– Способен настраивать правила фильтрации пакетов в компьютерных сетях (ПК-7)

---

Содержание дисциплины

---

Раздел 1. Введение.
Предмет и основные задачи дисциплины «Защита информации с помощью маршрутизаторов и коммутаторов», её значение в сис¬теме подготовке бакалавров по направлению «Инфокоммуникационные технологии и системы связи».
Раздел 2. Средства обеспечения безопасности инфраструктуры.
Рассмотрение средств обеспечения безопасности инфраструктуры. Листы доступа. Конфигурация различных типов листов доступа для коммутаторов. Технологии защиты коммутаторов от атак: DHCP Snooping, ARP Snooping, IP Source Guard. Протокол 802.1x и его компоненты. Протокол EAP, виды аутентификации пользователей посредством протокола EAP.
Раздел 3. Защита сети с помощью коммутаторов.
Механизмы обеспечения безопасности на уровне 2 модели OSI. Аутентификация и авторизация 802.1x. Динамическая привязка VLAN 802.1X.
Раздел 4. Защита сети с помощью маршрутизаторов.
Обзор основных методов защиты. Защита плоскости control. Защита плоскости

management. Защита плоскости data.
Раздел 5. Функции защиты данных в маршрутизирующей инфраструктуре.
Механизмы защиты процессора в маршрутизирующей инфраструктуре от распределенных атак в обслуживании (DDoS). Защита протоколов маршрутизации, конфигурирование листов доступа, внедрение механизмов качества обслуживания, выставление лимитов нагрузки процессора, памяти. Защита от подмены ip-адресов.
Раздел 6. Внедрение межсетевого экрана на основе зон и политик.
Установка и настройка межсетевого экрана (Zonebased policy firewall) на 2-4 уровнях модели OSI. Понятие зоны безопасности. Настройка политик межсетевого экрана. Настройка фильтрации продвинутого межсетевого экрана на 5-7 уровнях модели OSI.
Раздел 7. Архитектура и технологии построения VPN на базе IPsec.
Понятие виртуальной частной сети (VPN). Стек протоколов IPSec, алгоритмы шифрования, симметричная и ассиметричная криптография. Виды VPN. Внедрение виртуальных частных сетей на маршрутизаторе, используя виртуальные туннельные интерфейсы (VTI).
Раздел 8. Использование цифровых сертификатов для обеспечивания масштабируемой аутентификации VPN (PKI).
Понятие цифровых сертификатов. Применение алгоритмов ассиметричной криптографии для аутентификации VPN-пиров. Внедрение динамических VPN (DMVPN). Внедрение GET VPN.
Раздел 9. Архитектуры и технологий обеспечения удалённого доступа.
Рассмотрение архитектуры и технологий обеспечения удалённого доступа. Протоколы SSL/TLS. Внедрение удаленного доступа на базе SSL VPN. Внедрение удаленного доступа на базе Cisco Easy VPN. Дизайн, поиск и устранение неисправностей в сетях удаленного доступа.
Раздел 10. Контроль и предотвращение вторжений.
Технологии NAT и PAT. Zone-Based Policy Firewall и фильтрация URL. IPS.

---

Общая трудоемкость дисциплины

216 час(ов), 6 ЗЕТ

Форма промежуточной аттестации

Экзамен

### *Б1.В.ДВ.05.01 Общая физическая подготовка*

Цели освоения дисциплины

---

Целью преподавания дисциплины «Общая физическая подготовка» является: изучение и формирование физической культуры личности и способности направленного использования разнообразных средств физической культуры, спорта и туризма для сохранения и укрепления здоровья, психофизической подготовки и самоподготовки к будущей жизни и профессиональной деятельности.

---

Место дисциплины в структуре ОП

Дисциплина «Общая физическая подготовка» Б1.В.ДВ.05.01 является дисциплиной по выбору части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Физическая культура и спорт».

Требования к результатам освоения

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности (УК-7)

Содержание дисциплины

Раздел 1. Общая физическая и спортивная подготовка. Комплексное занятие
Общая физическая и специальная физическая подготовка. Комплексное занятие. Техника безопасности на занятиях по ОФП. Методика проведения комплексного занятия; Простейшие методики самооценки двигательной активности и суточных энергетических затрат. Повышение функциональных возможностей. Развитие основных физических качеств. Специальные контрольные упражнения, тесты ВСФК «ГТО»
Раздел 2. Ускоренное передвижение и легкая атлетика
Ускоренное передвижение и легкая атлетика. Методика индивидуального подхода и применения средств для направленного развития отдельных физических качеств. Упражнения для развития скоростно-силовых качеств, силовой выносливости, быстроты. Совершенствование техники бега. Прыжки и прыжковые упражнения
Раздел 3. Гимнастика и атлетическая подготовка
Гимнастика и атлетическая подготовка. Методы самоконтроля состояния здоровья, физического развития, функциональной подготовленности. Упражнения для развития ловкости, силы и силовой выносливости. Овладение техникой выполнения упражнений атлетической гимнастики
Раздел 4. Спортивные и подвижные игры
Спортивные и подвижные игры. Средства и методы мышечной релаксации в спорте. Основы методики организации судейства. Игры на месте, малоподвижные, подвижные, спортивные. Подвижные игры с использованием: общеразвивающих упражнений; прикладных упражнений; игровых заданий с элементами легкой атлетики, футбола, баскетбола, волейбола.
Раздел 5. Фитнес, функциональная тренировка
Фитнес, функциональная тренировка. Методы самооценки специальной физической и спортивной подготовленности. Воспитание необходимых физических качеств по видам и направлениям фитнеса

Раздел 6. Жизненно необходимые умения и навыки. Профессионально-прикладная физическая подготовка
Жизненно необходимые умения и навыки. Профессионально-прикладная физическая подготовка. Методики самостоятельного освоения отдельных элементов ППФП. Методика проведения производственной гимнастики с учетом заданных условий и характера труда. Совершенствование двигательных физических качеств, повышение функциональных возможностей. Формирование психической подготовленности

---

Общая трудоемкость дисциплины

328 час(ов),

Форма промежуточной аттестации

Зачет

***Б1.В.ДВ.05.02 Адаптационная физическая подготовка***

Цели освоения дисциплины

---

Целью преподавания дисциплины «Адаптационная физическая подготовка» является:
максимально возможное развитие жизнеспособности человека, имеющего отклонения в состоянии здоровья и обеспечение оптимального режима функционирования двигательных возможностей, духовных сил, их гармонизацию для самореализации в качестве социально и индивидуально значимого субъекта.

---

Место дисциплины в структуре ОП

---

Дисциплина «Адаптационная физическая подготовка» Б1.В.ДВ.05.02 является дисциплиной по выбору части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Физическая культура и спорт».

---

Требования к результатам освоения

---

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности (УК-7)

Содержание дисциплины

Раздел 1. Общая физическая и спортивная подготовка. Комплексное занятие
Общая физическая и специальная физическая подготовка. Комплексное занятие Техника безопасности на занятиях по ОФП. Методика проведения комплексного занятия; Простейшие методики самооценки двигательной активности и суточных энергетических затрат. Повышение функциональных возможностей. Развитие основных физических качеств
Раздел 2. Ускоренное передвижение и легкая атлетика
Ускоренное передвижение и легкая атлетика. Методика индивидуального подхода и применения средств для направленного развития отдельных физических качеств. Упражнения для развития скоростно-силовых качеств, выносливости, быстроты, гибкости с учетом данных контроля и самоконтроля. Совершенствование техники бега. Прыжки и прыжковые упражнения
Раздел 3. Гимнастика и атлетическая подготовка
Гимнастика и атлетическая подготовка. Методы самоконтроля состояния здоровья, физического развития, функциональной подготовленности. Дневник самоконтроля. Упражнения для развития ловкости, силы и выносливости. Овладение техникой выполнения упражнений атлетической гимнастики
Раздел 4. Спортивные и подвижные игры
Спортивные и подвижные игры. Средства и методы мышечной релаксации в спорте. Основы методики организации судейства. Игры на месте, малоподвижные, подвижные, спортивные (адаптивные формы). Подвижные игры с использованием: общеразвивающих упражнений; прикладных упражнений; игровых заданий с элементами легкой атлетики, футбола, баскетбола, волейбола с учетом данных контроля и самоконтроля
Раздел 5. Фитнес, функциональная тренировка
Фитнес, функциональная тренировка. Методы самооценки специальной физической и спортивной подготовленности. Воспитание необходимых физических качеств по видам и направлениям фитнеса с учетом данных врачебного контроля. Индивидуальный выбор оздоровительных систем физических упражнений
Раздел 6. Жизненно необходимые умения и навыки. Профессионально-прикладная физическая подготовка
Жизненно необходимые умения и навыки. Профессионально-прикладная физическая подготовка. Методики самостоятельного освоения отдельных элементов ППФП. Методика проведения производственной гимнастики с учетом заданных условий и характера труда. Совершенствование двигательных физических качеств, повышение функциональных возможностей. Формирование психической подготовленности

Общая трудоемкость дисциплины

328 час(ов),

Форма промежуточной аттестации

Зачет

***Б1.В.ДВ.05.03 Секции по видам спорта***

Цели освоения дисциплины

Целью преподавания дисциплины «Секции по видам спорта» является: изучение и формирование физической культуры личности и способности направленного использования разнообразных средств физической культуры, спорта и туризма для сохранения и укрепления здоровья, психофизической подготовки и самоподготовки к будущей жизни и профессиональной деятельности

Место дисциплины в структуре ОП

Дисциплина «Секции по видам спорта» Б1.В.ДВ.05.03 является дисциплиной по выбору части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Физическая культура и спорт».

Требования к результатам освоения

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности (УК-7)

Содержание дисциплины

Раздел 1. Общая физическая и спортивно-техническая подготовка. Комплексное занятие
Техника безопасности. Методика проведения комплексного занятия Простейшие методики самооценки двигательной активности и суточных энергетических затрат
Раздел 2. Ускоренное передвижение и легкая атлетика
Методика индивидуального подхода и применения средств для направленного развития отдельных физических качеств. Упражнения для развития физических качеств, необходимых в избранном виде спорта
Раздел 3. Гимнастика и атлетическая подготовка
Методы самоконтроля состояния здоровья, физического развития, функциональной подготовленности. Упражнения для развития ловкости, силы и силовой выносливости
Раздел 4. Спортивные и подвижные игры
Средства и методы мышечной релаксации в спорте. Основы методики организации судейства по избранному виду спорта. Овладение средствами спортивной тактики, техническими приемами в избранном виде спорта

Раздел 5. Фитнес, спортивная функциональная тренировка – «кроссфит»
Методы самооценки специальной физической и спортивной подготовленности по избранному виду спорта. Основные упражнения для тренировки по системе «кроссфит»
Раздел 6. Жизненно необходимые умения и навыки. Профессионально-прикладная физическая подготовка
Методики самостоятельного освоения отдельных элементов ППФП. Методика проведения производственной гимнастики с учетом заданных условий и характера труда. Совершенствование двигательных физических качеств, повышение функциональных возможностей в избранном виде спорта

---

Общая трудоемкость дисциплины

328 час(ов),

Форма промежуточной аттестации

Зачет

***Б1.В.ДВ.06.01 Безопасность управления техническими системами***

Цели освоения дисциплины

---

Целью преподавания дисциплины «Безопасность управления техническими системами» является:
формирование у студентов системы научных и профессиональных знаний и навыков в области организации и управления техническими системами применительно к решению задач технической эксплуатации автомобильного транспорта

---

Место дисциплины в структуре ОП

---

Дисциплина «Безопасность управления техническими системами» Б1.В.ДВ.06.01 является дисциплиной по выбору части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Защита информации в центрах обработки данных»; «Комплексная защита объектов информатизации».

---

Требования к результатам освоения

---

Процесс изучения дисциплины направлен на формирование следующих компетенций:

В соответствии с ФГОС:

– Способен оценивать технические возможности, анализировать угрозы и вырабатывать рекомендации по построению элементов информационно-телекоммуникационной инфраструктуры с учетом обеспечения требований информационной безопасности; (ОПК-13)
– Способен анализировать угрозы безопасности информации программного обеспечения (ПК-9)

---

Содержание дисциплины

---

Раздел 1. Технологический процесс как объект управления.
Структура и функции системы управления технологическими процессами (СУТП). Основные функциональные блоки систем автоматического управления (САУ). Локальные СУТП. Технические средства САР и их классификация по функциональному назначению
Раздел 2. Способы управления технологическим процессом.
Технические средства САР и их классификация по функциональному назначению
Раздел 3. Элементы проектирования систем автоматизации
Элементы структурных схем. Проектирование локальных систем. Функциональные схемы автоматизации. Выбор точек контроля, управления и сигнализации. Способы обозначения технологического оборудования и средств автоматизации. Выбор технических средств автоматизации.
Раздел 4. Элементы теории автоматического управления.
Математическое описание систем управления. Модели динамических управляемых объектов. Уравнение Лагранжа; дифференциальные уравнения типовых управляемых процессов и технических объектов. Установившиеся динамические процессы в технических системах.
Раздел 5. Системы автоматического регулирования.
Позиционные САР. Одноконтурные САР непрерывного действия. Типовые переходные процессы в САР. Качественные показатели переходных процессов. Типовые законы регулирования.

---

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

### *Б1.В.ДВ.06.02 Программы для ЭВМ и базы данных как объекты интеллектуальной собственности*

Цели освоения дисциплины

---

Целью преподавания дисциплины «Программы для ЭВМ и базы данных как объекты интеллектуальной собственности» является:
приобретение слушателями программы достаточных теоретических знаний и

практических навыков в сфере защиты интеллектуальной собственности, позволяющих обеспечить качественное нормативно-правовое обеспечение создания, становления и развития бизнеса, а также повышение уровня правовой культуры.

Место дисциплины в структуре ОП

Дисциплина «Программы для ЭВМ и базы данных как объекты интеллектуальной собственности» Б1.В.ДВ.06.02 является дисциплиной по выбору части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Введение в профессию»; «Гуманитарные аспекты информационной безопасности»; «Документоведение».

Требования к результатам освоения

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– Способен использовать методы и средства криптографической защиты информации при решении задач профессиональной деятельности; (ОПК-10)
– Способен противодействовать угрозам безопасности информации с использованием встроенных средств защиты информации операционных систем (ПК-3)

Содержание дисциплины

Раздел 1. Интеллектуальная собственность как правовой институт
Результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации, охраняемые в РФ как интеллектуальная собственность. Интеллектуальные права. Интеллектуальные права и вещные права. Автор результата интеллектуальной деятельности. Исключительное право на результат интеллектуальной деятельности. Договор об отчуждении исключительного права на результат интеллектуальной деятельности. Лицензионный договор на результат интеллектуальной деятельности, его виды. Сублицензионный договор.
Раздел 2. Авторское право и смежные права
Автор произведения науки, литературы и искусства и его права. Действие исключительного права на произведения науки, литературы и искусства на территории РФ. Автор произведения науки, литературы и искусства. Соавторство. Объекты авторских прав. Переводы, иные производные произведения. Составные произведения. Программы для ЭВМ. Государственная регистрация программ для ЭВМ и баз данных. Право авторства и право автора на имя. Право на неприкосновенность произведения и защита

произведения от искажений. Исключительное право на произведение. Знак охраны авторского права. Свободное воспроизведение произведения в личных целях. Свободное использование произведения в информационных, научных, учебных или культурных целях. Свободное использование произведения библиотеками, архивами и образовательными организациями. Право пользователя программы для ЭВМ и базы данных. Срок действия исключительного права на произведение. Переход произведения в общественное достояние. Служебное произведение. Произведения, создаваемые в рамках гражданско-правовых договоров. Объекты смежных прав. Знак правовой охраны смежных прав. Права на исполнение. Право на фонограмму. Право организаций эфирного и кабельного вещания. Право изготовителя базы данных. Право публикатора на произведение науки, литературы или искусства. Гражданско-правовая, административная и уголовная ответственность за нарушение авторских и смежных прав.

---

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

### 3. Аннотации программ практик

***производственной Б2.В.01.01(П) Эксплуатационная практика***

Цели проведения практики

---

Целью проведения практики «Эксплуатационная практика» является: закрепление и углубление теоретических знаний; формирование и развитие профессиональных знаний; приобретение практических навыков; формирование компетенций, а также приобретение опыта самостоятельной профессиональной и научной деятельности, необходимых для последующей профессиональной деятельности.

Эта цель достигается путем решения следующих(ей) задач(и):

- закрепление на практике знаний и умений, полученных в процессе теоретического обучения;
- развитие профессиональных навыков;
- ознакомление с общей характеристикой объекта практики и правилами техники безопасности;

Место практики в структуре ОП

«Эксплуатационная практика» Б2.В.01.01(П) входит в блок 2 учебного плана, который относится к части, формируемой участниками образовательных отношений, и является обязательной составной частью образовательной программы по направлению «10.05.02 Информационная безопасность телекоммуникационных систем».

«Эксплуатационная практика» опирается на знания, полученные при изучении предшествующих дисциплин, а также на знания и практические навыки, полученные при прохождении практик(и) «Научно-исследовательская работа».

Требования к результатам освоения

В процессе прохождения практики студент формирует и демонстрирует следующие компетенции:

– Способен формулировать задачи, планировать и проводить исследования, в том числе эксперименты и математическое моделирование объектов, явлений и процессов телекоммуникационных систем, включая обработку и оценку достоверности их результатов; (ОПК-12)
– Способен оценивать технические возможности, анализировать угрозы и вырабатывать рекомендации по построению элементов информационно-телекоммуникационной инфраструктуры с учетом обеспечения требований информационной безопасности; (ОПК-13)
– Способен проводить инструментальный мониторинг качества обслуживания и анализ защищенности информации от несанкционированного доступа в телекоммуникационных системах и сетях в целях управления их функционированием; (ОПК-15)
– Способен проектировать защищенные телекоммуникационные системы и их элементы, проводить анализ проектных решений по обеспечению заданного уровня безопасности и требуемого качества обслуживания телекоммуникационных систем, разрабатывать необходимую техническую документацию с учетом действующих нормативных и методических документов, проводить подготовку исходных данных для технико-экономического обоснования соответствующих проектных решений; (ОПК-16)
– Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни (УК-6)

Содержание практики

Раздел 1. Согласование темы индивидуального задания
Выбор и согласование темы с научным руководителем.
Раздел 2. Составление индивидуального плана работы студента
Определение и согласование индивидуального плана работы.
Раздел 3. Выполнение индивидуального задания
Получение и выполнение индивидуального задания.

Раздел 4. Подготовка отчета
Оформление и подготовка работы.
Раздел 5. Защита отчета
Выступление и защита работы.

---

Общая трудоемкость дисциплины

324 час(ов), 9 ЗЕТ

Форма промежуточной аттестации

Зачет

***производственной Б2.В.01.02(Н) Научно-исследовательская работа***

Цели проведения практики

---

Целью проведения практики «Научно-исследовательская работа» является: закрепление и углубление теоретических знаний; формирование и развитие профессиональных знаний; приобретение практических навыков; формирование компетенций, а также приобретение опыта самостоятельной профессиональной и научной деятельности, необходимых для последующей профессиональной деятельности.

Эта цель достигается путем решения следующих(ей) задач(и):

- закрепление на практике знаний и умений, полученных в процессе теоретического обучения;
- развитие профессиональных навыков;
- ознакомление с общей характеристикой объекта практики и правилами техники безопасности;
- планирование исследования (выбор темы, обоснование необходимости, определение целей и задач, выдвижение гипотез, формирование программы, подбор средств и инструментария);
- проведение исследования (изучение литературы, сбор, обработка и обобщение данных, объяснение полученных результатов и новых фактов, аргументирование, формулировка выводов);
- оформление отчета о результатах исследования (изучение нормативных требований, формирование структуры и содержания, написание, редактирование, формирование списка использованных источников информации, оформление приложений);
- выступление с докладами на студенческих конференциях по результатам

исследований.

Место практики в структуре ОП

«Научно-исследовательская работа» Б2.В.01.02(Н) входит в блок 2 учебного плана, который относится к части, формируемой участниками образовательных отношений, и является обязательной составной частью образовательной программы по направлению «10.05.02 Информационная безопасность телекоммуникационных систем».

«Научно-исследовательская работа» опирается на знания, полученные при изучении предшествующих дисциплин, а также на знания и практические навыки, полученные при прохождении практик(и) «Ознакомительная практика».

Требования к результатам освоения

В процессе прохождения практики студент формирует и демонстрирует следующие компетенции:

– Способен формулировать задачи, планировать и проводить исследования, в том числе эксперименты и математическое моделирование объектов, явлений и процессов телекоммуникационных систем, включая обработку и оценку достоверности их результатов; (ОПК-12)
– Способен оценивать технические возможности, анализировать угрозы и вырабатывать рекомендации по построению элементов информационно-телекоммуникационной инфраструктуры с учетом обеспечения требований информационной безопасности; (ОПК-13)
– Способен проводить инструментальный мониторинг качества обслуживания и анализ защищенности информации от несанкционированного доступа в телекоммуникационных системах и сетях в целях управления их функционированием; (ОПК-15)
– Способен проектировать защищенные телекоммуникационные системы и их элементы, проводить анализ проектных решений по обеспечению заданного уровня безопасности и требуемого качества обслуживания телекоммуникационных систем, разрабатывать необходимую техническую документацию с учетом действующих нормативных и методических документов, проводить подготовку исходных данных для технико-экономического обоснования соответствующих проектных решений; (ОПК-16)
– Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни (УК-6)

Содержание практики

Раздел 1. Согласование темы индивидуального задания
Выбор темы, из списка представленного научным руководителем и последующее согласование.
Раздел 2. Составление индивидуального плана работы студента

Согласование индивидуального плана работ с научным руководителем.
Раздел 3. Выполнение индивидуального задания
Выполнение индивидуального задания.
Раздел 4. Подготовка отчета
Предоставление предварительного отчета научному руководителю для согласования.
Раздел 5. Защита отчета
Проведение зачета по практике с последующим ответом на вопросы согласно с выбранной теме.

---

Общая трудоемкость дисциплины

144 час(ов), 4 ЗЕТ

Форма промежуточной аттестации

Зачет

***учебной Б2.О.01.01(У) Ознакомительная практика***

Цели проведения практики

---

Целью проведения практики «Ознакомительная практика» является: закрепление и углубление теоретических знаний; формирование и развитие профессиональных знаний; приобретение практических навыков; формирование компетенций, а также приобретение опыта самостоятельной профессиональной и научной деятельности, необходимых для последующей профессиональной деятельности.

Эта цель достигается путем решения следующих(ей) задач(и):

- закрепление на практике знаний и умений, полученных в процессе теоретического обучения;
- развитие профессиональных навыков;
- ознакомление с общей характеристикой объекта практики и правилами техники безопасности;

---

Место практики в структуре ОП

---

«Ознакомительная практика» Б2.О.01.01(У) входит в блок 2 учебного плана, который относится к обязательной части, и является обязательной составной частью образовательной программы по направлению «10.05.02 Информационная

безопасность телекоммуникационных систем».

«Ознакомительная практика» опирается на знания, полученные при изучении предшествующих дисциплин.

---

Требования к результатам освоения

---

В процессе прохождения практики студент формирует и демонстрирует следующие компетенции:

– Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности; (ОПК-2)
– Способен формулировать задачи, планировать и проводить исследования, в том числе эксперименты и математическое моделирование объектов, явлений и процессов телекоммуникационных систем, включая обработку и оценку достоверности их результатов; (ОПК-12)
– Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни (УК-6)

---

Содержание практики

---

Раздел 1. Согласование темы индивидуального задания
Выбор и согласование темы с научным руководителем.
Раздел 2. Составление индивидуального плана работы студента
Определение и согласование индивидуального плана работы.
Раздел 3. Выполнение индивидуального задания
Получение и выполнение индивидуального задания.
Раздел 4. Подготовка отчета
Оформление и подготовка работы.
Раздел 5. Защита отчета
Выступление и защита работы.

---

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

***производственной Б2.О.02.01(Пд) Преддипломная практика***

Цели проведения практики

---

Целью проведения практики «Преддипломная практика» является: закрепление и углубление теоретических знаний; формирование и развитие профессиональных знаний; приобретение практических навыков; формирование компетенций, а также приобретение опыта самостоятельной профессиональной и научной деятельности, необходимых для последующей профессиональной деятельности.

Эта цель достигается путем решения следующих(ей) задач(и):

- закрепление на практике знаний и умений, полученных в процессе теоретического обучения;
- развитие профессиональных навыков;
- ознакомление с общей характеристикой объекта практики и правилами техники безопасности;
- подбор необходимых материалов для выполнения выпускной квалификационной работы (или магистерской диссертации).

---

Место практики в структуре ОП

---

«Преддипломная практика» Б2.О.02.01(Пд) входит в блок 2 учебного плана, который относится к обязательной части, и является обязательной составной частью образовательной программы по направлению «10.05.02 Информационная безопасность телекоммуникационных систем».

«Преддипломная практика» опирается на знания и практические навыки полученные при изучении дисциплин и прохождении всех типов практик. «Преддипломная практика» является завершающей в процессе обучения и предшествует выполнению выпускной квалификационной работы.

---

Требования к результатам освоения

---

В процессе прохождения практики студент формирует и демонстрирует следующие компетенции:

– Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности; (ОПК-2)
– Способен формулировать задачи, планировать и проводить исследования, в том числе эксперименты и математическое моделирование объектов, явлений и процессов телекоммуникационных систем, включая обработку и оценку достоверности их результатов; (ОПК-12)

– Способен оценивать технические возможности, анализировать угрозы и вырабатывать рекомендации по построению элементов информационно-телекоммуникационной инфраструктуры с учетом обеспечения требований информационной безопасности; (ОПК-13)
– Способен проводить инструментальный мониторинг качества обслуживания и анализ защищенности информации от несанкционированного доступа в телекоммуникационных системах и сетях в целях управления их функционированием; (ОПК-15)
– Способен проектировать защищенные телекоммуникационные системы и их элементы, проводить анализ проектных решений по обеспечению заданного уровня безопасности и требуемого качества обслуживания телекоммуникационных систем, разрабатывать необходимую техническую документацию с учетом действующих нормативных и методических документов, проводить подготовку исходных данных для технико-экономического обоснования соответствующих проектных решений; (ОПК-16)
– Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни (УК-6)

---

Содержание практики

---

Раздел 1. Согласование темы индивидуального задания
Выбор и согласование темы с научным руководителем.
Раздел 2. Составление индивидуального плана работы студента
Определение и согласование индивидуального плана работы.
Раздел 3. Выполнение индивидуального задания
Получение и выполнение индивидуального задания.
Раздел 4. Подготовка отчета
Оформление и подготовка работы.
Раздел 5. Защита отчета
Выступление и защита работы.

---

Общая трудоемкость дисциплины

540 час(ов), 15 ЗЕТ

Форма промежуточной аттестации

Зачет

**4. Аннотация программы ГИА**

***«Государственная итоговая аттестация»***

Цели и задачи дисциплины

---

Целью государственной итоговой аттестации является определение соответствия результатов освоения студентами основной профессиональной образовательной программы высшего образования требованиям федерального государственного образовательного стандарта (далее ФГОС ВО) по направлению

подготовки (специальности) «10.05.02 Информационная безопасность телекоммуникационных систем», ориентированной на на следующие виды деятельности:
- научно-исследовательский
- проектный
- контрольно-аналитический
- организационно-управленческий
- эксплуатационный.

---

Место дисциплины в структуре ОП

---

В соответствии с учебным планом государственная итоговая аттестация проводится в конце последнего года обучения. При условии успешного прохождения всех установленных видов итоговых аттестационных испытаний, входящих в итоговую государственную аттестацию, выпускнику присваивается соответствующая квалификация.

---

Требования к результатам освоения

---

Программа ГИА направлена на оценку результатов освоения обучающимися образовательной программы и степени овладения следующими профессиональными компетенциями (ПК):
В соответствии с ФГОС:

– Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства; (ОПК-1)
– Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности; (ОПК-2)
– Способен использовать математические методы, необходимые для решения задач профессиональной деятельности; (ОПК-3)
– Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования радиоэлектронной техники, применять физические законы и модели для решения задач профессиональной деятельности; (ОПК-4)
– Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации; (ОПК-5)
– Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в процессе функционирования сетей электросвязи в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю; (ОПК-6)
– Способен создавать программы на языке высокого уровня, применять существующие реализации структур данных и алгоритмов; (ОПК-7)

– Способен применять методы научных исследований при проведении разработок в области функционирования, развития и обеспечения информационной безопасности телекоммуникационных систем и сетей; (ОПК-8)
– Способен использовать программные, программно-аппаратные и технические средства защиты информации при решении задач профессиональной деятельности; (ОПК-9)
– Способен формировать, внедрять и обеспечивать функционирование системы менеджмента информационной безопасности телекоммуникационных систем и сетей; (ОПК-9.1)
– Способен реализовывать комплекс организационных мероприятий по обеспечению информационной безопасности и устойчивости телекоммуникационных систем и сетей; (ОПК-9.2)
– Способен проводить мониторинг защищенности сетевых ресурсов и формировать отчеты по выявленным уязвимостям; (ОПК-9.3)
– Способен использовать методы и средства криптографической защиты информации при решении задач профессиональной деятельности; (ОПК-10)
– Способен применять положения теории в области электрических цепей, радиотехнических сигналов, распространения радиоволн, кодирования, электрической связи, цифровой обработки сигналов для решения задач профессиональной деятельности; (ОПК-11)
– Способен формулировать задачи, планировать и проводить исследования, в том числе эксперименты и математическое моделирование объектов, явлений и процессов телекоммуникационных систем, включая обработку и оценку достоверности их результатов; (ОПК-12)
– Способен оценивать технические возможности, анализировать угрозы и вырабатывать рекомендации по построению элементов информационно-телекоммуникационной инфраструктуры с учетом обеспечения требований информационной безопасности; (ОПК-13)
– Способен применять технологии и технические средства сетей электросвязи; (ОПК-14)
– Способен проводить инструментальный мониторинг качества обслуживания и анализ защищенности информации от несанкционированного доступа в телекоммуникационных системах и сетях в целях управления их функционированием; (ОПК-15)
– Способен проектировать защищенные телекоммуникационные системы и их элементы, проводить анализ проектных решений по обеспечению заданного уровня безопасности и требуемого качества обслуживания телекоммуникационных систем, разрабатывать необходимую техническую документацию с учетом действующих нормативных и методических документов, проводить подготовку исходных данных для технико-экономического обоснования соответствующих проектных решений; (ОПК-16)
– Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма (ОПК-17)
– Способен формулировать и настраивать политики безопасности операционных систем (ПК-1)
– Способен оценивать угрозы безопасности информации операционных систем (ПК-2)
– Способен противодействовать угрозам безопасности информации с использованием встроенных средств защиты информации операционных систем (ПК-3)
– Способен устанавливать и настраивать антивирусные средства защиты информации в операционных системах (ПК-4)
– Способен проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах (ПК-5)
– Способен оценивать угрозы безопасности информации в компьютерных сетях (ПК-6)
– Способен настраивать правила фильтрации пакетов в компьютерных сетях (ПК-7)
– Способен конфигурировать и контролировать корректность настройки программно-аппаратных средств защиты информации в компьютерных сетях (ПК-8)
– Способен анализировать угрозы безопасности информации программного обеспечения (ПК-9)

– Способен формулировать и обосновывать правила безопасной эксплуатации программного обеспечения (ПК-10)
– Способен осуществлять мероприятия по противодействию угрозам безопасности информации, возникающим при эксплуатации программного обеспечения (ПК-11)
– Способен проводить специальные исследования на побочные электромагнитные излучения и наводки технических средств обработки информации (ПК-12)
– Способен проводить контроль защищенности информации от утечки за счет побочных электромагнитных излучений и наводок (ПК-13)
– Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий (УК-1)
– Способен управлять проектом на всех этапах его жизненного цикла (УК-2)
– Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели (УК-3)
– Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия (УК-4)
– Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия (УК-5)
– Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни (УК-6)
– Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности (УК-7)
– 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-8)
– Способен принимать обоснованные экономические решения в различных областях жизнедеятельности (УК-10)
– Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности (УК-11)

---

Содержание

---

Подготовка и защита выпускной квалификационной работы

---

Общая трудоемкость дисциплины

216 час(ов), 6 ЗЕТ