**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:

формирование систематизированных знаний об основных закономерностях и особенностях исторического процесса, определение места россииской цивилизации в мировом историческом процессе с учетом стремления к объективности в его освещении; формирование гражданскои позиции.

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 историю
Теория и методология исторической науки. История как наука: предмет, цели, задачи изучения. Сущность, формы и функции исторического знания. Исторический источник: понятие и классификация. Виды источников. Методология истории. Историография истории. История России как неотъемлемая часть всемирной истории. Великое переселение народов. Восточные славяне в древности: теории этногенеза славян; историко-географические аспекты формирования восточных славян. Общественно-политический строй, экономика и верования восточных славян.
Раздел 2. Русские земли и средневековый мир (V- XV вв.)
Средневековье как этап всемирной истории. Периодизация и региональная специфика

средневековья. От Древней Руси к Московскому государству (IX- XV вв.). Древнерусское государство. Социокультурное значение принятия византийского формата христианства. Киевская Русь во второй половине XI - начале XII вв. Раздробленность русских земель и ее последствия. Формирование и особенности государственных образований на территории Древней Руси. Иноземные нашествия в XIII в. Русь и Орда. Русь и Запад. Объединительные процессы в русских землях (XIV- середина XV вв.). Возвышение Москвы.Образование Московского государства (вторая половина XV-начало XVI вв.). Внутренняя и внешняя политика Ивана III и его преемников. Освобождение от ордынской зависимости. Борьба с Великим княжеством Литовским за «наследство» Киевской Руси. Культура Руси-России.

Раздел 3. Россия и мир в XVI–XVIII вв.

Россия и мир в XVI-XVII вв. Новое время как особая фаза всемирно-исторического процесса. Начало разложения феодализма и складывания капиталистических отношений. Религиозный фактор в политических процессах. Абсолютизм. Начало правления Ивана IV. Реформы Избранной Рады. Опричнина. Внешняя политика Ивана Грозного. «Смутное время». Правление первых Романовых. Россия в XVII в.: на пути к абсолютизму. Бунташный век. Внешняя политика России (1613-1689). Культура России (XVI-XVII вв.). Россия и мир в XVIII вв. Великая французская революция. Образование США. Предпосылки, цели, характер осуществления реформ Петра I. Формирование сословной системы организации общества. Основные направления внешней политики России первой четверти XVIII в. Обретение Россией статуса империи. Эпоха дворцовых переворотов. Правление Екатерины II: внешняя и внутренняя политика. Россия на рубеже XVIII - XIX вв. Правление Павла I. Культура России (XVIII в.).

Раздел 4. Россия и мир в XIX-начале XX вв.

Становление индустриального общества. Промышленный переворот в странах Запада и его последствия. Образование колониальных империй. Россия в первой половине XIX в.: внешняя и внутренняя политика России (Александр I, Николай I). Российская империя во второй половине XIX - начале XX вв. Политика Александра II и Александра III. Внешняя политика России во второй половине XIX в. Общественные движения в России (XIX в.): декабристы, консерваторы, либералы, революционеры. Модернизация России на рубеже веков. С. Ю. Витте. Кризис раннего индустриального общества и его последствия. Борьба за передел мира. Политическая система России в начале XX в. и ее развитие. Внешняя политика России в конце XIX – начале XX вв. Революция 1905- 1907 гг.: причины, события, итоги. П.А.Столыпин. Первая мировая война как проявление кризиса цивилизации XX в. Россия в условиях первой мировой войны и нарастания общенационального кризиса. Культура России XIX- начала XX вв.

Раздел 5. Россия и мир в XX – начале XXI вв.

Великая российская революция: 1917- 1922. Февраль 1917 г. и его итоги. Октябрь 1917 г. Россия в годы Гражданской войны и интервенции. Образование СССР. Советская модернизация: основные этапы и направления. Внешняя политика (1920-е- 1940-е гг.). Новая экономическая политика (нэп). Советская политическая система и ее особенности. Советская внешняя политика в межвоенное десятилетие. СССР во второй мировой и Великой Отечественной войнах. Антигитлеровская коалиция. Итоги войны. Россия и мир во второй половине XX в. «Холодная война». СССР в послевоенный период (1945-1985). «Перестройка». Внешняя политика. Нарастание центробежных сил и распад СССР. 5.4. Постсоветская Россия и мир (конец XX- начало XXI вв.). Крушение биполярного мира и его последствия. Российская Федерация: 1991-1999. Российская Федерация на современном этапе. Культура современной России.

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. Физическая культура в профессиональной подготовке студентов и спортивная подготовка студентов в образовательном процессе.
Физическая культура в профессиональной подготовке студентов и социокультурное развитие личности студента. Социально-биологические основы адаптации организма человека к физической и умственной деятельности, факторам среды обитания. Образ жизни и его отражение в профессиональной деятельности. Общая физическая и спортивная подготовка студентов в образовательном процессе. Методические основы самостоятельных занятий физическими упражнениями и самоконтроль в процессе занятий. Профессионально-прикладная физическая подготовка будущих специалистов

(ППФП)
Раздел 2. Базовый комплекс занятий по общей физической подготовке
Упражнения для развития основных физических качеств. Совершенствование координационных способностей
Раздел 3. Комплекс занятий по общей физической подготовке
Упражнения для развития выносливости, силы, ловкости, быстроты, гибкости. Использование подвижных спортивных игр.

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:
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. Учебно-познавательная сфера общения
Студенческая жизнь в России и за рубежом. Высшее образование в России и за рубежом. История и традиции моего вуза.
Раздел 2. Социально-культурная сфера общения
Язык как средство межкультурного общения. Охрана окружающей среды. Экологически чистые ИКТ. Плюсы и минусы глобализации. Проблемы глобального языка и культуры.
Раздел 3. Профессиональная сфера общения. Современные ИКТ: общие проблемы
Информационные технологии. Научно-технический прогресс и его достижения в сфере инфокоммуникационных технологий и систем связи. Плюсы и минусы всеобщей информатизации общества. .
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 общества

Общая трудоемкость дисциплины

360 час(ов), 10 ЗЕТ

Форма промежуточной аттестации

Экзамен

Б1.О.04 Экономика

Цели освоения дисциплины

Целью преподавания дисциплины «Экономика» является:
сформулировать у студентов экономическое мировоззрение, умение анализировать экономические ситуации и закономерности поведения экономических субъектов в условиях рыночной экономики.

Место дисциплины в структуре ОП

Дисциплина «Экономика» Б1.Б.05 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 «История связи».

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. Введение в экономическую науку
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
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.
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. Налогово-бюджетная политика и мультипликатор
Мультипликатор государственных расходов, налоговый мультипликатор.

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.Б.06 является одной из дисциплин базовой 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. Что есть философия?
Что есть философия? понятие философии, ее особое положение среди других наук. Генезис философии. Что есть философия? (часть 2): структура философии (основные философские науки). Категории, принципы и законы философии. Функции философии. Понятие мировоззрения, типы мировоззрения. Основные проблемы философии. Основные философские направления.
Раздел 2. История философии
Философия древности: досократики, Софисты и Сократ: основание философии западной морали, Платон: основание философского идеализма, Аристотель: первая систематизация знаний, стоицизм и неоплатонизм, Философия Средневековья: патристика и схоластика, Философия эпохи Возрождения, Новоевропейская наука и метафизика, Критическая философия И.Канта, Диалектика Г.Гегеля и марксизма, Современная западная философия, Отечественная философия
Раздел 3. Философия бытия
Развитие понятия бытия (от Парменида до Гегеля). Понятие материи и его развитие от античного материализма до марксизма. Понятия движения, пространства и времени. Понятие идеи, его диалектика и математические начала онтологии от Пифагора до Гейзенберга.
Раздел 4. Сознание и познание
Сознание как духовное выражение действительности. Генезис сознания. Идеальность сознания, проблема идеального. Сознание и самосознание. Социальная сущность сознания и исторические формы мышления.
Раздел 5. Научное познание
Понятие науки, ее развитие. Понятие субъекта и объекта научного знания. Понятие научного базиса. Предмет и объект научного знания. Эмпирический и теоретический уровни познания. Понятие научного факта, гипотезы и теории. Основные принципы научного исследования. Научная картина мира. Структура научных революций Т. Куна. Сциентизм и антисциентизм. Диалектика научной истины. Состав научного знания.
Раздел 6. Философия человека
Общие представления о философской антропологии. Природа и личность. Роль человеческой личности в истории. Человек как совокупность общественных отношений и его биологическая природа. Внеисторический характер человеческой личности. Антропология религиозная и эпохи позитивизма. Проблема этического начала личности и способы его нивелирования в современном обществе.
Раздел 7. Социальная философия
Личность и общество. Предмет социальной философии. Понятие общества и его структура. Понятие социальной реальности. Состав социальной реальности и основные сферы общественной жизни. Проблема происхождения государства. Основные признаки государства. Гражданское общество и государство.

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: формирование знаний, умений и навыков, позволяющих проводить самостоятельный анализ проблем, возникающих в различных областях профессиональной деятельности.

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. Дифференциальное исчисление функции одной переменной
Функция. Предел. Сравнение бесконечно малых. Непрерывность функции в точке и на отрезке. Классификация точек разрыва. Понятие производной. Теоремы о среднем. Правило Лопиталя. Производные высших порядков. Исследование функции одной переменной.
Раздел 2. Интегральное исчисление функции одной переменной
Понятие первообразной. Техника интегрирования. Задачи, решаемые с помощью определённого интеграла. Свойства определённого интеграла. Несобственный интеграл. Понятие сходимости.
Раздел 3. Функции многих переменных.
Частные производные. Особенности исследования функции многих переменных. Производная по направлению и градиент. Дивергенция и ротор
Раздел 4. Кратные интегралы
Двойной интеграл, понятие и приложения. Вычисление двойного интеграла в декартовых и полярных координатах. Понятие о тройном интеграле.
Раздел 5. Криволинейные интегралы.
Криволинейные интегралы первого и второго типов. Условие независимости криволинейного интеграла от пути интегрирования. Формула Грина. Вычисление криволинейных и поверхностных интегралов непосредственно и с использованием формул Остроградского –Гаусса и Стокса.
Раздел 6. Дифференциальные уравнения.
Понятие дифференциального уравнения. Постановка задачи Коши, существование и единственность решений. Методы решения дифференциальных уравнений различных типов. Основные положения теории линейных дифференциальных уравнений.
Раздел 7. Теория рядов.
Числовой ряд и его сумма. Признаки сходимости числовых рядов. Функциональные ряды. Степенной ряд, его свойства, операции над сходящимися степенными рядами. Ряды Тейлора и Маклорена. Тригонометрический ряд. Понятие ортонормированной системы функций. Ряды Фурье
Раздел 8. Интегральные преобразования.
Преобразование Фурье, свойства прямого и обратного преобразований. Оператор Лапласа, его свойства. Методы нахождения изображений и оригиналов. Решение задач операторным методом.
Раздел 9. Элементы теории поля
Векторное поле. Его характеристики. Понятие потока векторного поля.

Общая трудоемкость дисциплины

288 час(ов), 8 ЗЕТ

Форма промежуточной аттестации

Зачет, Экзамен

Б1.О.07.02 Теория вероятностей и математическая статистика

Цели освоения дисциплины

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

овладение навыками и умениями построения математических моделей инфокоммуникационных процессов и объектов

Место дисциплины в структуре ОП

Дисциплина «Теория вероятностей и математическая статистика» Б1.Б.12.03 является базовой дисциплиной цикла учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Изучение дисциплины «Теория вероятностей и математическая статистика» 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:

– способностью применять соответствующий математический аппарат для решения профессиональных задач (ОПК-2)

Содержание дисциплины

Раздел 1. Случайные события
Основные понятия теории вероятностей. События. Вероятность события. Статистический подход к описанию случайных явлений. Непосредственное определение вероятностей. Элементы комбинаторики. Размещения, перестановки, сочетания. Алгебра событий. Аксиомы теории вероятностей. Основные теоремы теории вероятностей: теорема сложения вероятностей, теорема умножения вероятностей, формула полной вероятности, теорема гипотез (формула Байеса). Последовательность независимых испытаний. Распределение Пуассона. Локальная и интегральная теоремы Муавра-Лапласа
Раздел 2. Случайные величины
Дискретные случайные величины. Распределение дискретной случайной величины. Непрерывные случайные величины. Плотность случайной величины. Функция распределения. Числовые характеристики случайных величин. Математическое ожидание. Моменты второго порядка. Закон равномерной плотности. Закон Пуассона. Одномерное нормальное распределение.
Раздел 3. Многомерные случайные величины
Системы случайных величин (случайные векторы). Функция распределения. Условные законы распределения. Зависимые и независимые случайные величины. Числовые

характеристики системы двух случайных величин. Корреляционный момент. Коэффициент корреляции. Нормальный закон на плоскости. Вероятность попадания в область произвольной формы.

Раздел 4. Предельные теоремы теории вероятностей

Предельные теоремы теории вероятностей. Неравенство Чебышева. Закон больших чисел. Теорема Бернулли. Центральная предельная теорема

Раздел 5. Цепи Маркова

Основные понятия теории случайных процессов. Марковские процессы. Свойства и вероятные характеристики

Раздел 6. Математическая статистика

Основные задачи математической статистики. Статистическая функция распределения. Статистический ряд. Гистограмма. Обработка опытов. Оценки для математического ожидания и дисперсии. Доверительные интервалы и доверительные вероятности. Выравнивание статистических рядов. Критерии согласия (Пирсона, Фишера, Колмогорова, Стьюдента).

Раздел 7. Методы изучения статистических зависимостей

Понятие корреляции. Оценки тесноты связи. Регрессионный анализ. Статистический анализ моделей.

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
Действия с комплексными числами в алгебраической форме. Модуль и аргумент. Особенности применения тригонометрической и показательной форм комплексного числа. Основная теорема алгебры. Извлечение корня из комплексного числа. Обзор элементарных функций комплексного переменного.
Раздел 2. Алгебра матриц
Понятие матрицы. Действия с матрицами. Решение матричных уравнений. Ранг матрицы. Собственные числа
Раздел 3. Определители
Методы вычисления определителей, их свойства. Минор.
Раздел 4. Системы линейных алгебраических уравнений
Решение систем методом Гаусса. Теоремы Крамера. Теорема Кронекера-Капелли. Особенности решения однородных систем
Раздел 5. Аналитическая геометрия на плоскости и в пространстве
Линейные геометрические объекты и работа с ними. Кривые и поверхности второго порядка. Использование квадратичных форм.
Раздел 6. Линейное пространство произвольной размерности. Линейные операторы
Понятие линейного пространства произвольной размерности. Линейный оператор и его свойства.

Общая трудоемкость дисциплины

180 час(ов), 5 ЗЕТ

Форма промежуточной аттестации

Экзамен

Б1.О.07.04 Дискретная математика

Цели освоения дисциплины

Целью преподавания дисциплины «Дискретная математика» является:
формирование у студентов фундаментальных знаний в области дискретного анализа и выработка практических навыков по применению дискретной математики в программировании и инфокоммуникационных технологиях.

Место дисциплины в структуре ОП

Дисциплина «Дискретная математика» Б1.Б.12.02 является базовой дисциплиной цикла учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Изучение дисциплины «Дискретная математика» 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. Множества и операции над ними.
Множества и операции над ними. Отношения и функции. Высказывания.
Раздел 2. Булевы функции.
Булевы функции. Нормальные формы формул. ДНФ и КНФ, СДНФ и СКНФ. Минимизация булевых функций.
Раздел 3. Понятия о предикатах и кванторах. Полнота и замкнутость. Полные системы булевых функций.
Понятия о предикатах и кванторах. Полнота и замкнутость. Полные системы булевых функций
Раздел 4. Комбинаторика
Элементы комбинаторики. Размещения, перестановки, сочетания. Комбинаторные схемы. Производящие функции
Раздел 5. Теории графов.
Основные понятия и определения теории графов. Алгоритмы поиска кратчайших путей между вершинами графа. Методы решения оптимизационных задач на графах.
Раздел 6. Транспортные сети.
Транспортные сети. Алгоритм построения максимального потока в транспортной сети
Раздел 7. Алгоритмы.
Понятия конечных автоматов. Основы теории решеток

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:
изучение основных закономерностей обмена информацией на расстоянии, обработки, эффективной передачи и помехоустойчивого приёма в технических и естественных системах различного назначения и формирования фундаментальных знаний основ теории детерминированных и случайных аналоговых и цифровых сигналов и систем их преобразования, основ потенциальной помехоустойчивости и оптимального приема сигналов в каналах с помехами, принципов и методов многоканальной передачи, хранения, распределения и приема дискретных и непрерывных сообщений, аналоговых и цифровых методов модуляции, методов повышения энергетической и спектральной эффективности систем электросвязи базирующихся на фундаменте теории информации, эффективного и помехоустойчивого кодирования, способствовать развитию творческих способностей студентов, умению формулировать и решать задачи оптимизации систем связи, умению творчески применять и самостоятельно повышать свои знания в области инфотелекоммуникаций, в том числе космической, оптической и многоканальной специальной связи..

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. 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, молекулярной физики, 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.Б.13.01 является базовой дисциплиной цикла 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 и динамика поступательного и вращательного движения. Работа и энергия. Законы сохранения в механике. Элементы специальной теории относительности.
Раздел 2. Молекулярная физика и термодинамика
Распределения Максвелла-Больцмана. Средняя энергия молекул. Первое начало термодинамики. Работа при изопроцессах. Второе начало термодинамики. Энтропия. Циклы.

Раздел 3. Электричество
Электростатическое поле в вакууме и в веществе. Законы постоянного тока.
Раздел 4. Магнитное поле в вакууме
Магнитные силы. Магнитные поля, создаваемые токами.
Раздел 5. Магнетизм и электромагнетизм
Магнитные свойства вещества.Явление электромагнитной индукции. Уравнения Максвелла.
Раздел 6. Колебания и волны
Свободные и вынужденные колебания. Сложение гармонических колебаний. Волны. Уравнение волны. Энергия волны. Перенос энергии волной. Электромагнитные волны.

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.Б.13.02 является одной из дисциплин базовой 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
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. Спектральные представления колебаний в ЭЦ.
временными характеристиками ЭЦ. 3 7 Раздел 7. Спектральные представления колебаний в ЭЦ. Анализ спектрального состава периодических негармонических колебаний с помощью ряда Фурье. Спектр амплитуд и спектр фаз периодического колебания. Анализ режима периодического колебания в ЭЦ. Мощность периодического негармонического колебания. Представление непериодического колебания интегралом Фурье. Комплексная спектральная плотность. Одностороннее преобразование Фурье. Частотный метод анализа переходных колебаний в цепях. Условия безыскаженной передачи сигналов через ЭЦ.
Раздел 8. Нелинейные резистивные цепи.
Общая характеристика и классификация нелинейных элементов и цепей. Анализ резистивной цепи с одним нелинейным двухполюсником в режиме постоянного тока. Нахождение рабочей точки по однозначной и многозначной ВАХ. Статические и дифференциальные параметры. Анализ нелинейной ЭЦ при гармоническом воздействии.

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: сформировать необходимый минимум специальных теоритических 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 будующей 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 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 .

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. Системы счисления. Модели решения функциональных и вычислительных задач
Системы счисления. Моделирование как метод познания. Объект, субъект, цель моделирования. Классификация моделей. Цели, задачи, решаемые с помощью моделей. Методы и технологии моделирования. Основные понятия и методы теории информации и кодирования. Сигналы, данные, информация. Общая характеристика процессов сбора, передачи, обработки и накопления информации.
Раздел 2. Технические средства реализации информационных процессов
Современные технические средства, построенные по принципу архитектуры ЭВМ (планшеты, мобильные устройства и т.д.)
Раздел 3. Методы управления средствами передачи информации
Классификация, назначение операционных систем (ОС). Операционные системы: Windows, Linux и др. Особенности, отличия, интересы, области применения
Раздел 4. Средства и методы передачи информации
Сетевые технологии обработки данных. Режимы передачи данных в компьютерных сетях. Типы синхронизации данных при передаче и способы передачи информации. Аппаратные средства, применяемые при передаче данных. Основы компьютерной коммуникации. Принципы построения и основные топологии вычислительных сетей, коммуникационное оборудование. Физическая передающая среда ЛВС и методы доступа к ней. Сетевой сервис и сетевые стандарты. Программы для работы в сети Интернет. Защита информации в локальных и глобальных компьютерных сетях. Шифрование данных. Электронная подпись."
Раздел 5. Программные средства реализации информационных процессов
Служебные программы, утилиты. Драйверы. Архиваторы. Антивирусные программы. Встроенные программы. Прикладное программное обеспечение. ППО 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: ознакомление слушателей с основными возможностями языка программирования С++.

Место дисциплины в структуре ОП

Дисциплина «Языки программирования» Б1.О.09.02 является дисциплиной обязательной части учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Изучение дисциплины «Языки программирования» 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. Основы С++
Основные понятия языка С++: типы данных, указатели, массивы, условные операторы, логические операторы, циклы, создание функции, математические функции. Структура

программы на С++. Модульное построение программы. Инструментарий для разработки программ на С++.
Раздел 2. Работа со строками
Создание строк, обработка, сравнение, объединение стандартными средствами С++. Разбор специального класса String для работы со строками.
Раздел 3. Работа с файлами
Создание текстового файла, открытие, редактирование, сохранение, поиск по файлу с помощью средств языка С++. Работа с бинарными файлами.
Раздел 4. Функции
Объявление и определение функции, вызов функции, параметры функции, область видимости и время жизни переменных. Перегрузка функции.
Раздел 5. Введение в объектно-ориентированное программирование
Понятие структуры. Определение понятии класса, объекта класса, методы классов. Закрытая, открытая часть класса. Доступ к полям классов. Принципы объектно-ориентрованного программирования.

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:
Целью преподавания дисциплины является изучение вопросов основ построения документооборота. Дисциплина «Документоведение» должна обеспечивать формирование фундамента подготовки будущих специалистов 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 «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. Система норм права, регулирующих деятельность телекоммуникаций в РФ
В рамках раздела изучается система норм права, регулирующих деятельность телекоммуникаций, в РФ. Субординация норм права. Конституционные основы деятельности в телекоммуникациях РФ
Раздел 2. Система норм права, регулирующих деятельность документооборота организации в РФ

В рамках раздела изучается система норм права, регулирующих деятельность в области документооборота 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

В рамках раздела изучаются следующие вопросы: 1. Федеральная связь РФ и ее состав. 2. Сеть связи общего пользования. 3. Выделенные сети связи. 4. Технологические сети связи. 5. Сети связи специального назначения. 6. Государственное регулирование деятельности в области связи. 7. Обязанности операторов связи в соответствии с федеральным законом РФ "О связи". 8. Универсальные услуги связи. 9. Подача жалоб и предъявление претензий и их рассмотрение. Место предъявления претензий. 10. 12. 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

В рамках раздела изучаются термины и определения, основные понятия рассмотриваемые 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

В рамках раздела основные понятия и положения рассматриваемые в ФЗ "О персональных данных".

Раздел 6. Правовые основы ограничения доступа к информации

В рамках раздела 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.

В рамках раздела изучаются 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.

В рамках раздела изучаются основные понятия и положения рассматриваемые в ФЗ "Об электронной подписи». Основные положения ГОСТа Р 34.10-2012.

Раздел 9. Основы DLP-систем

В рамках раздела изучаются основные понятия и положенияDLPсистем. 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

В рамках раздела изучаются 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.
Введение в информационные технологии, основные определения. Классификация ИТ. Информационные процессы реализации информационных технологий. Технологический процесс поиска, сбора и этапы обработки информации. Основные свойства ИТ. Методы анализ и синтеза информации. Теория формализации. Государственная программа цифровизации.
Раздел 2. Современные технические средства взаимодействия мобильных информационных систем
Классификация программных средств (ПС) для мобильных и стационарных систем. Операционная система Android. Архитектура, функции Android. Классификация технических средств под управлением ОС Android Операционная система iOS Архитектура, функции iOS Классификация технических средств под управлением ОС iOS. Характеристика ОС: KaiOS, Sailfish OS (Аврора ОС).
Раздел 3. Информационные технологии конечного пользователя
Автоматизация информационных процессов, автоматизированные системы управления,

принципы построения и функционирования. Организационные формы обработки информации в АСУ. Классификация АСУ. Виды обеспечения АСУ. Автоматизированное рабочее место оператора (АРМ). Моделирование функциональных задач. Основные определения. Классификация моделей, методов моделирования и принципы их построения. Базы данных (БД), классификация. Проектирование баз данных.

Раздел 4. Информационные технологии в глобальных, локальных и корпоративных сетях

Базовые принципы построения корпоративных сетей и их сопровождения. Проектно-техническая организация работы. Информационные системы. Назначение и классификация. Корпоративные информационные системы. Виды корпоративных информационных систем. Проектно-техническая организация работы по проектированию корпоративной сети. Принципы организации работы web-порталов различного назначения

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 Интернет

Веб-технологии. URL, DNS, Типы DNS-серверов. 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.
Раздел 2. Устройство персонального компьютера
Основные и дополнительные компоненты персонального компьютера.
Раздел 3. Процессор
Назначение, устройство и принцип работы процессора. Характеристики процессора. Особенности использования процессора.
Раздел 4. Увеличение быстродействия процессора. Система охлаждения процессора.
Методы увеличения производительности процессора. Модернизация процессора и особенности его эксплуатации. Соблюдение теплового режима. Виды теплоотводов. Причины перегрева ЦП.
Раздел 5. Системная плата
Назначение и компоненты системной платы. Чипсеты системных плат. Внутренние и внешние интерфейсы системной платы.
Раздел 6. Оперативная память. Видеоадаптеры.
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.
Раздел 7. Звуковое обеспечение. Накопители информации
Звуковые платы. Принципы функционирования и характеристики звуковой платы. Накопители на жёстких магнитных дисках. Сменные накопителей на основе flash памяти.

Накопители на оптических дисках. Интерфейсы накопителей информации
Раздел 8. Блок питания. Монитор.
Назначение, принципы работы и характеристики блока питания ПК. Выбор блока питания ПК. Назначение, типы и основные характеристики мониторов. Принципы работы СКЕ и LCD мониторов, принципы работы плазменных и OLED мониторов.
Раздел 9. Устройства ввода информации. Клавиатура. Мышь.
Устройства ввода информации. Манипулятор типа мышь. Графический планшет.
Раздел 10. Заключение
Перспективные направления проектирования вычислительных устройств.
Вычислительные кластеры. Аппаратные средства для распределенных вычислений.

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 «Защита информации в компьютерных сетях»; «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)
– Способен использовать программные, программно-аппаратные и технические средства защиты информации при решении задач профессиональной деятельности; (ОПК-9)

Содержание дисциплины

Раздел 1. Основные принципы построения современных инфокоммуникационных сетей. Эволюция технологий.
Тенденции развития инфокоммуникаций. Услуги в инфокоммуникациях. Классификация сетевых технологий. Модели ISO/OSI, TCP/IP, NGN. Организации, стандартизирующие решения в области телекоммуникаций. Особенности построения и развития сетей связи в РФ
Раздел 2. Технология TCP/IP: протокол IP.
0IP версий 4 и 6. Адресация, распределение адресного пространства, распределение адресов, DNS, структура заголовков, алгоритм обработки пакета на узле.
Раздел 3. Маршрутизация в IPсетях.
Понятие маршрутизации. Внешняя и внутренняя маршрутизация. Формирование таблиц маршрутизации. Понятие автономной системы. Типы маршрутизаторов. Принципы построения маршрутизаторов. Алгоритм Белмана-Форда. Алгоритм Дейстры. Понятие метрики. Основные протоколы маршрутизации: RIP, OSPF, IS-IS, BGP.
Раздел 4. Технологии уровня доступа.
Эволюция Ethernet: от 10 Мбит/с к 10 Гбит/с. Особенности формирования кадра Ethernet: уровни LLC и MAC. Метод доступа CSMA/CD. Формат кадра Ethernet. Протокол ARP. Коммутаторы Ethernet: неуправляемые и управляемые. Требования к неблокирующему режиму работы коммутатора. Способы организации неблокирующего коммутатора. СКС для Ethernet: виды кабеля, разъемов, обжимка. Использование сетей PON для организации доступа абонентов. Использование существующей телефонной линии: xDSL, протокол PPP.
Раздел 5. Технологии транспортных сетей.
Рабочая среда E1. Формирование PDH. Технология SDH – формирование нагрузки, использование для организации магистрали. Понятие синхронизации. Технология ATM для построения транспортных сетей. Технология DWDM, принципы волнового мультиплексирования. Технология MPLS.
Раздел 6. Методы управления сетью.
Функции транспортного уровня, управление трафиком на транспортном уровне. Протокол UDP. Протокол TCP. Установление соединения. Квитирование. Медленный старт. Алгоритм RED и его влияние на работу TCP. Версии TCP. Влияние протоколов транспортного уровня на работу приложений. Управление сетевыми элементами. Протокол SNMP. Маршрутизация как способ управления сетью.
Раздел 7. Беспроводные сети связи.

Классификация беспроводных сетей. Беспроводные технологии доступа. Сотовые сети, особенности построения. Процедура идентификации абонента. Принципы организации беспроводных каналов на магистральных участках и в труднодоступных районах.
Раздел 8. Услуги в NGN и качество обслуживания.
Классификация услуг в NGN. Требования к услугам: показатели качества обслуживания, стандарты и рекомендации. Качество обслуживания и качество восприятия. Источники ухудшения качества услуги. IPтелефония и IPTV как примеры мультисервисных услуг: проблемы и их решения.
Раздел 9. Обработка и хранение информации в глобальных сетях.
Управление информационными потоками в глобальных сетях, хранение информации, в т.ч. распределенное. Архитектура центров обработки данных. Распределенные облачные вычисления

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:
изучение вопросов управления информационной безопасностью

Место дисциплины в структуре ОП

Дисциплина «Основы информационной безопасности» Б1.О.10.01 является дисциплиной обязательной части учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Изучение дисциплины «Основы информационной безопасности» 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 методы научных исследований при проведении разработок в области функционирования, развития и обеспечения информационной безопасности телекоммуникационных систем и сетей; (ОПК-8)

Содержание дисциплины

Раздел 1. Оценка рисков информационной безопасности
Основные составляющие информационной безопасности. Угрозы информационной безопасности в информационных системах. 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 безопасности информационных 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 «этический хакинг». 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

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:

1. Формирование у обучаемых умения ориентироваться в нормативно-правовом поле деятельности отрасли связи и ее хозяйствующих субъектов. Представления о теоретических основах сферы обращения информации и ее правового регулирования в РФ.

Место дисциплины в структуре ОП

Дисциплина «Организационное и правовое обеспечение информационной безопасности» Б1.О.10.02 является дисциплиной обязательной части учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Изучение дисциплины «Организационное и правовое обеспечение информационной безопасности» 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 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. Подача жалоб и предъявление претензий и их рассмотрение. Место предъявления претензий. Управление сетями связи в чрезвычайных ситуациях и в условиях чрезвычайного положения. Основные положения Устава и Конвенции Международного союза электросвязи.
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. Виды информации в зависимости от категории доступа и в зависимости от порядка ее предоставления или распространения. Право на доступ к информации. Ограничение доступа к информации. Порядок ограничения доступа к информации, распространяемой с нарушением авторских и (или) смежных прав. Защита информации в соответствии с законом РФ "Об информации, информационных технологиях и о защите информации". Обязанности организатора распространения информации в сети "Интернет". Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации.
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. Условия прекращения допуска должностного лица или гражданина к государственной тайне. Ограничения прав должностного лица или гражданина, допущенных или ранее допускавшихся к государственной тайне. Ответственность за разглашение государственной тайны в РФ.
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. Требования, являющиеся

обязательными к письменной форме согласия субъекта персональных данных на обработку его персональных данных. Специальные категории персональных данных и перечень оснований для их обработки. Дисциплинарная, административная и уголовная ответственность за нарушение законодательства РФ о 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

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:

Изучение студентами основных принципов построения и анализа криптографических средств защиты информации, а также навыков и умения в применении знаний для конкретных условий.

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».

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. Основные понятия
Криптография. Цели криптографии. История развития криптографии. Классификация криптографических методов. Обеспечение конфиденциальности, целостности, неотказуемости, аутентичности, неотслеживаемости информации. Основные понятия: шифр, открытый текст, шифртекст, электронная подпись, хэш-функция,
Раздел 2. Основные характеристики шифров
Алгебраическая модель шифра. Алгебраическая модель шифра замены. Алгебраическая модель шифра перестановки. Алгебраическая модель шифра гаммирования
Раздел 3. Симметричная криптография. Электронная подпись
Классификация симметричных криптографических систем. Требования к блочным шифрам. Требования к поточным шифрам. Криптографические параметры узлов и блоков блочных шифров. Базовые криптографические преобразования блочных шифров. Способы реализации блочных шифров. Процедура развертывания ключа.

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:

Целью преподавания дисциплины является изучение вопросов основ защиты информации в телекоммуникационных системах. Дисциплина «Программноаппаратные средства защиты информации» должна обеспечивать формирование фундамента подготовки будущих бакалавров 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 «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 «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. Основы микропроцессорной техники
Трехшинная архитектура микроЭВМ, Архитектуры микропроцессоров 8080, формат и система команд микропроцессоров 8080 и 8085
Раздел 2. Методы ввода-вывода
Классификация регистров памяти и методов ввода-выводов, программный ввод-вывод с/без квитированием, память типа FIFO
Раздел 3. Установка и настройка Arduino в ОС Windows
Установка Arduino IDE, Запуск Arduino IDE, Подключение Arduino к компьютеру, Настройка Arduino IDE на работу с ArduinoUno, загрузка скетчей, Среда разработки AtmelStudio
Раздел 4. Классификация типов программно-аппаратных средств защиты информации
Идентификация и аутентификация, управление доступом, протоколирование и аудит, криптография, экранирование.
Раздел 5. Методы построения программно-аппаратных средств защиты информации
Обзор методов построения: 1. Средств, разработанных для защиты информации от НСД в информационных сетях, но допускающие применение и в персональных компьютерах; 2. Средств, принципиально применимых только в компьютерных сетях и предназначенные для разделения информационных потоков, — так называемые межсетевые экраны; 3. Средств, принципиально предназначенных для защиты информации от НСД в персональных компьютерах.

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:

Целью преподавания дисциплины 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 инженернотехнических 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 «Защита в операционных системах».

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

<u>Раздел 1. Введение</u>
Предмет, цели, задачи и содержание курса инженернотехнической защиты информации (ИТЗИ). Роль и место курса в подготовке специалистов поорганизации защиты информации в государственных и коммерческих структурах. Базовые знания,

необходимые для изучения курса. Рекомендуемые учебные пособия

Раздел 2. Объекты информационной защиты

Виды информации, защищаемой техническими средствами. Свойства информации, влияющие на возможности ее защиты. Понятие о демаскирующих признаках объектов защиты. Показатели качества информации. Старение информации. Полезность и цена информации. Классификация демаскирующих признаков. Опознавательные признаки и признаки деятельности объектов. Понятие об источниках, носителях и получателях информации. Классификация источников информации. Понятие об опасном сигнале и их источниках. Основные и вспомогательные технические средства и системы. Побочные электромагнитные излучения и наводки.

Раздел 3. Технические средства охраны объектов инфокоммуникаций

Роль и место технических средств в организации режима охраны объектов инфокоммуникаций, современная концепция защиты объектов инфокоммуникаций. Основные составляющие систем ТСО: датчики, приборы визуального наблюдения, системы сбора и обработки информации, средства связи, питания и тревожновызывной сигнализации; практическая реализация систем ТСО: охрана режимных помещений, проект охраны объектов.

Раздел 4. Способы и средства добывания информации техническими средствами. Технические каналы утечки информации

Способы и средства добывания информации техническими средствами на объектах инфокоммуникаций. Способы и средства наблюдения. Способы и средства наблюдения в оптическом диапазоне. Способы и средства наблюдения в радиодиапазоне. Способы и средства перехвата сигналов. Способы и средства подслушивания. Способы и средства добывания информации о радиоактивных веществах. Технические каналы утечки информации. Особенности утечки информации. Характеристики технических каналов утечки информации. Оптические каналы утечки информации. Радиоэлектронные каналы утечки информации. Акустические каналы утечки информации. Материально-вещественные каналы утечки информации. Комплексирование технических каналов утечки информации.

Раздел 5. Методология проектирования и моделирования инженерно-технической защиты объектов инфокоммуникаций.

Системный подход к инженерно-технической защите информации и объектов инфокоммуникаций. Основные этапы проектирования системы защиты объектов инфокоммуникаций техническими средствами. Принципы моделирования объектов защиты и технических каналов утечки информации. Способы оценки угроз безопасности информации и расходов на техническую защиту объектов инфокоммуникаций. Способы и принципы работы средств защиты объектов инфокоммуникаций от наблюдения, подслушивания и перехвата. Организационные и технические меры инженерно-технической защиты объектов инфокоммуникаций в государственных и коммерческих структурах; контроль эффективности защиты информации. Оптимизация проекта системы (предложений) защиты информации и объектов инфокоммуникаций. Требования к оформлению проекта системы (предложений) при представлении на согласование и утверждений.

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 основные сведения об этике новых отношений, учитывающих массовую компьютеризацию всех сторон жизни и деятельности личности, общества и государства, о социально-правовых проблемах информатизации и обеспечения информационной безопасности, о современных научных направлениях, связанных с решением этих проблем.

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

<u>Раздел 1. Место и роль проблем информационной безопасности в становлении современного информационного общества</u>
Нормативные документы в области информационной безопасности. Структура и задачи органов, обеспечивающих ИБ. Гуманитарная сущность ИБ.
<u>Раздел 2. Проблемы обеспечения баланса интересов личности, общества и государства в информационной сфере</u>

Закон "О безопасности". Состояние защищенности. Задача установления приемлемого баланса интересов. Правовое урегулирование отношений

Раздел 3. Ценностная ориентация личности, ее информационное обоснование и информационная безопасность

Основные компоненты ИБ в области культуры. Особенности современных информационных компаний. Модели взаимодействия участников социального взаимодействия. Анализ материалов социальных сетей и СМИ

Раздел 4. Основы компьютерной этики

Проблемы, связанные с разработкой моральных кодексов для компьютерных профессионалов и простых пользователей, чья работа связана с использованием компьютерной техники. Проблемы защиты прав собственности, авторских прав, права на личную жизнь и свободу слова применительно к области информационных технологий. Группа проблем, связанных с появлением компьютерных преступлений

Раздел 5. Компьютерные правонарушения

Виды компьютерных правонарушений: использование вредоносного ПО, взлом паролей, кража персональных данных, фишинг, распространение противоправной информации. Уголовная ответственность в странах мира

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. Неприкосновенность частной жизни

Конституция РФ Статья 23(часть1), Конституция РФ Статья 24

Раздел 8. Риски использования информационных технологий

Понятие рисков в сфере информационных технологий. Риски, вызванные утечкой информации и использованием ее конкурентами или сотрудниками в целях, которые могут навредить. 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:

Цель преподавания дисциплины - познакомить студентов с современными концепциями управления проектами, показать связь между управлением проектами и финансовым менеджментом, маркетингом, управлением персоналом и стратегиями развития компании. Познакомить с технологиями и инструментарием в сфере управления проектами. Дисциплина «Основы управления проектами» должна обеспечивать формирование фундамента

подготовки бакалавров, 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 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. Теоретические основы проектной деятельности
Определение проекта. Его основные характеристики и измерения. Элементы проектной деятельности. Классификация проектов. Содержание и процессы управления проектами.
Раздел 2. Технология проектной деятельности: жизненный цикл проекта, его основные этапы
Методология и методика предпроектного анализа (анализ ситуации). Управление интеграцией (содержанием) проекта. Мобилизация ресурсов проекта.
Раздел 3. Разработка и управление ресурсными подсистемами проекта
Управление временем проекта. Управление стоимостью проекта. Управление качеством проекта. Управление командой проекта. Управление коммуникациями проекта. Управление рисками проекта.
Раздел 4. Мониторинг реализации проекта
Мониторинг и контроль работ проекта. Мониторинг коммуникаций. Мониторинг рисков.
Раздел 5. Управление изменениями
План и контроль изменений. Интегрированный контроль изменений.
Раздел 6. Оценка эффективности реализации проекта и завершение проекта
Оценка и управление стоимостью проекта. Оценка и управление качеством. Ключевые

показатели эффективности проекта. Закрытие проекта.

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. 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 управленияинформационной 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 информационноаналитических 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.

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 операционных систем. Дисциплина «Защищенные операционные системы» 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 дисциплиной обязательной части учебного плана подготовки специалитета по направлению «10.05.02 Информационная безопасность телекоммуникационных систем». Изучение дисциплины «Защита в операционных системах» 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 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. История развития операционных систем.
История разработки ОС MSDOS, Windows и Unix.Версии ОС. Установка и модернизация Windows Server. Введение в Server Core.
Раздел 2. Система управления доступом в ОС MS Windows.
Основные компоненты ОС MS Windows. Модель операционной системы. Различие между клиентской и серверной версии. Системные процессы, драйвера, ядро. Вводится понятие реестр операционной системы. Управление сервисами и процессами. Система журналирования
Раздел 3. Роли ОС MS Windows Server. Реализация доменных служб ActiveDirectory.
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. Роли ОС MS Windows Server. Реализация доменных служб 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. Групповая политика.
Раздел 5. Хранилище Windows Server.
Многоуровневые пространства хранения. Создание пространств хранения. Ограничения пулов хранения. Создание виртуального диска. Работа с iSCSI хранилищами. Общие папки NFS и CIFS.
Раздел 6. Реализация системы безопасности сети в ОС MS Windows.
Утилиты по настройке сети. Угрозы сетевой безопасности, реализация брандмауэров. Настройка брандмауэра Windows. Защита доступа к сети.
Раздел 7. Дополнительные возможности Active Directory.
Сайты в ActiveDirectory. Миграция, слияние и модификация ActiveDirectory. Центр сертификации.

Раздел 8. Внедрение программ обеспечения безопасности в ОС MS Windows.
Установка дополнительной системы защиты информации, для упрощения управлением доступом к файлам, на примере системы SearchInform.

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: Изучение вопросов основ криптографической защиты информации в телекоммуникационных системах.

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 «Математические основы 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:

изучение методов и средств построения и эксплуатации беспроводных технологий для обеспечения информационной безопасности на объекте, а также на изучение основных подходов к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию технологий защиты передачи информации в беспроводных коммуникациях.

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 «Защита в операционных системах»; «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. Сетевые атаки
Стадии проведения сетевой атаки. Классификации сетевых угроз, уязвимостей и атак. Атаки на реализации сетевых протоколов, отдельные узлы и службы. Основные механизмы проведения сетевых атак на различных уровнях модели ISO/OSI. Проблемы обеспечения конфиденциальности, целостности и доступности информации на различных уровнях модели ISO/OSI
Раздел 2. Механизмы реализации атак в сетях TCP/IP
Удаленное определение версии ОС с использованием особенностей реализации стека протоколов TCP/IP. Методы сканирования портов. Методы обнаружения пакетных сниферов. Методы обхода МЭ
Раздел 3. Методы перехвата сетевых соединений в сетях TCP/IP
Имперсонация вслепую. Десинхронизация TCP-соединений. Атаки, направленные на сетевую инфраструктуру
Раздел 4. Примеры сетевых атак в сетях TCP/IP. Технические меры защиты от сетевых атак
Принуждение к ускоренной передаче. Атаки, направленные на отказ в обслуживании. Изменение конфигурации и состояния хостов. Недостатки протоколов семейства TCP/IP с точки зрения обеспечения безопасности информации. Технические меры защиты от

сетевых атак
Раздел 5. Криптографические протоколы обеспечения безопасности
Протоколы аутентификации на прикладном уровне. Протокол Kerberos. Протоколы аутентификации на транспортном уровне. Протокол SSL/TLS. Достоинства и недостатки аутентификации на различных уровнях модели ISO/OSI
Раздел 6. Защита виртуальных частных сетей (VPN)
Назначение, основные возможности, принципы функционирования и варианты реализации VPN. Организация туннелирования на различных уровнях модели ISO/OSI. Достоинства и недостатки применения VPN. Протокол IPSEC. Протоколы AH и ESP. Особенности работы протокола IPSEC в туннельном и транспортном режимах. Протокол управления ключами ISAKMP/Oakley. Использование протокола L2TP для организации виртуальных частных сетей
Раздел 7. Разработка защищенных сетевых приложений
Аутентификация, шифрование, обеспечение целостности с использованием программного интерфейса SSPI. Программный интерфейс Open SSL
Раздел 8. Средства защиты локальных сетей при подключении к Интернет
Межсетевые экраны (МЭ). Место и роль МЭ в обеспечении сетевой безопасности. Классификация МЭ. Требования к МЭ. Основные возможности и схемы развертывания МЭ. Достоинства и недостатки МЭ. Построение правил фильтрации. Методы сетевой трансляции адресов (NAT). Шлюзы уровня приложений. Реализация сетевой политики безопасности с использованием МЭ. Методы обхода межсетевых экранов
Раздел 9. Средства и методы предотвращения и обнаружения вторжений
Системы обнаружения вторжений (СОВ). Назначение и возможности средств обнаружения вторжений на хосты, протоколы и сетевые службы. Место и роль средств обнаружения вторжений в общей системе обеспечения сетевой безопасности. Классификация СОВ. Выявление атак на основе сигнатур атак и выявления аномалий. Аудит прикладных служб. Средства обнаружения уязвимостей сетевых служб. Способы противодействия вторжениям. Системы виртуальных ловушек (Honey Pot и Padded Cell)

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:

Знакомство с основными методами и средствами обеспечения защиты информации при проектировании и использовании электронных баз данных.

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

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:

изучение студентами принципов построения безопасных инфокоммуникационных систем и сетей, их базовых типов, основных протоколов межсетевого взаимодействия, методов адресации сетевых устройств на физическом, логическом и прикладном уровнях.

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. Введение

Предмет и основные задачи дисциплины «Основы проектирования защищенных инфокоммуникационных систем», её значение в системы подготовке бакалавров по направлению «Информационная безопасность».

Раздел 2. Определение функций сети. Классификация сетей. Модель OSI. Общие сведения о модели обмена данными между хостами.

Определение основных понятий. История развития локальных сетей. Проблемы объединенных сетей. Классификация инфокоммуникационных сетей по размеру, топологии, физической среде передачи данных. Возникновение и задачи эталонной модели взаимодействия открытых систем. Уровни модели OSI и их взаимодействие.

Раздел 3. Понятие Ethernet. Применение технологии коммутации в сетях

Технология Ethernet. Структуры сетей Ethernet. Формат кадра Ethernet. IEEE 802.3. Механизм предотвращения коллизий CSMA/CD. Передача и прием кадров, управление потоком. Многоскоростные сети Ethernet. Принципы работы коммутатора. Организация виртуальных локальных сетей VLAN. Разделение ресурсов в локальной сети. Access и trunk-порты коммутаторов. Инкапсуляция dot1q. Методы предотвращение широковещательных штормов в сети. Работа протокола SpanningTree. Настройка механизмов защиты на коммутаторах.

Раздел 4. Беспроводные локальные сети (WLAN). Понятие безопасности WLAN. Обеспечение WLAN.

Основы работы беспроводных сетей: топологии построения беспроводных сетей, принципы распространения радиоволн, основы теории антенн, технологию прямого расширения спектра, регулирующие организации, стандарты и сертификации, а так же беспроводные технологии, не относящиеся к 802.11, и их влияние.

Раздел 5. Обзор функций маршрутизации, протокол IP, Организация CIDR и VLSM подсетей. Маршрутизация. Включение статической маршрутизации.

Схема IP-адресации. Поля параметров IP-пакета. Формат IP-адреса. Реальные и транслируемые адреса. Принципы адресации в глобальной сети Internet. Маска подсети, расчет маски переменной длины.

Раздел 6. Протоколы TCP и UDP, DHCP, DNS, Понятие технологий удаленных подключений.

Протоколы TCP и UDP. Основные поля TCP и UDP пакетов. Флаги TCP. Трехэтапное установление связи TCP. Поток TCP и управление плавающим окном передачи сообщений. Номера портов TCP и UDP. Адресация данных для прикладного уровня сетевых устройств.

Раздел 7. Управление сетевой средой. Обнаружение соседних устройств в сети. Управление устройствами Cisco

CiscoDiscoveryProtocol (CDP) – протокол обнаружения соседних устройств сети. Анализ получаемой информации. Протоколы удаленного подключения к устройствам.

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:

формирование компетентности в области разработки комплексной системы защиты информации предприятия

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 «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

<u>Раздел 1. Введение в дисциплину. Сущность комплексной системы защиты информации и принципы ее организации</u>
Цель, задачи дисциплины, значение ее для подготовки специалиста. Знания и умения студентов, которые должны быть получены в результате ее изучения. Понятие, сущность и назначение комплексной системы защиты информации, ее задачи для обеспечения деятельности предприятия. Принципы организации комплексной системы защиты информации.
<u>Раздел 2. Методологические и концептуальные основы комплексной системы защиты информации.</u>

Методология защиты информации и ее основные задачи. Уровень обеспечения безопасности информации. Достаточность защиты информации. Варианты построения комплексной системы защиты. Основные факторы, влияющие на организацию комплексной системы защиты информации. Характер и степень влияния различных факторов на организацию системы защиты информации.

Раздел 3. Определение и нормативное закрепление информации ограниченного доступа.

Классификация информации по видам тайны и степеням конфиденциальности. Этапы работы по выявлению состава защищаемой информации. Нормативное закрепление состава 11 защищаемой информации. Порядок организации нормативного закрепления информации ограниченного доступа.

Раздел 4. Определение состава объектов защиты.

Понятие объекта защиты. Последовательность определения объекта защиты. Значение носителей защищаемой информации как объектов защиты. Факторы, определяющие состав носителей информации. Сущность защищаемого объекта информатизации. Методика выявления состава носителей защищаемой информации. Основные и вспомогательные технические средства и системы. Особенности помещений как объектов защиты

Раздел 5. Источники, способы и результаты дестабилизирующего воздействия на информацию.

Определение источников дестабилизирующего воздействия на информацию. Модель формирования множества дестабилизирующих факторов. Понятие угрозы безопасности информации. Базовая модель угроз безопасности информации. Классификация угроз безопасности информации для объекта информатизации. Анализ и оценка угроз информационной безопасности объекта.

Раздел 6. Выявление каналов утечки и методов несанкционированного воздействия на информацию.

Сущность утечки информации и несанкционированного воздействия на информацию. Структурная модель канала утечки информации. Технические каналы утечки информации и их классификация. Модель технических каналов утечки информатизации на типовом объекте информатизации. Каналы утечки из-за несанкционированного воздействия на информацию на системы, использующие информационно - коммуникационные технологии. Инсайдерские каналы утечки информации и социальный инжиниринг Методы социального инжиниринга.

Раздел 7. Моделирование процессов защиты информации.

Понятие модели и объекта моделирования. Основные виды моделей и их характеристика. Задачи и этапы моделирования в процессе построения комплексной системы защиты информации. Понятие архитектуры системы защиты информации. Кибернетическая, функциональная, информационная и организационная модели комплексной системы защиты информации. Формальные модели безопасности. Теории и методы моделирования процессов защиты информации.

Раздел 8. Технологическое и организационное построение комплексной системы защиты информации.

Общее содержание работ по организации комплексной системы защиты информации. Характеристика технологического и организационного направлений создания комплексной системы защиты информации. Содержание стадий построения комплексной системы защиты информации. Предпроектное обследование. Назначение и структура технического задания, техникоэкономического обоснования. Технический проект, рабочий проект. Апробация системы защиты информации и ввод ее в эксплуатацию.

Раздел 9. Кадровое, материальнотехническое и нормативно-методическое обеспечение

защиты информации
Кадровое обеспечение функционирования комплексной системы защиты информации. Защита человеческих ресурсов. Распределение функций по защите информации. Материально-техническое обеспечение защиты информации. Нормативно- методическое обеспечение комплексной защиты информации на предприятии. Порядок разработки нормативных и организационнораспорядительных документов, регламентирующих работу по защите информации на предприятии.
Раздел 10. Планирование и контроль комплексной системы защиты информации.
Понятие, принципы и методы планирования комплексной системы защиты информации. Стадии планирования. Факторы, влияющие на выбор принципов и способов планирования. Структура и общее содержание планов предприятия и функционирования комплексной системы защиты информации. Организация выполнения планов. Сущность, цель, задачи и содержание контроля комплексной системы защиты информации. Виды и методы контроля системы защиты информации. Основные контрольные мероприятия по защите информации
Раздел 11. Оценка эффективности комплексной системы защиты информации
Понятие эффективности и эффективности защиты информации. Требование по защите информации. Показатель и норма эффективности защиты информации. Подходы к оценке эффективности систем защиты информации и их особенности. Состав методов и моделей оценки эффективности систем защиты информации. Области применения различных методов и моделей для решения задач оценки эффективности системы защиты информации на предприятии. Методики проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.
Раздел 12. Аттестация объектов информатизации по требованиям безопасности информации.
Состав и содержание нормативно - правовых актов по аттестации объектов информатизации. Система аттестации объектов информатизации по требованиям безопасности информации. Организация аттестационных испытаний. Типовое содержание аттестационных испытаний объектов информатизации. Аттестационные испытания автоматизированных систем на соответствие требованиям по защите информации от несанкционированного доступа Аттестационные испытания объектов вычислительной техники по требованиям безопасности информации от утечки по каналам побочных электромагнитных излучений и наводок. Аттестационные испытания выделенных помещений. Инструментальные средства для проведения аттестационных испытаний. Основы проведения поисковых мероприятий по выявлению закладочных устройств.

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 инфокоммуникационных сетей и систем, а также изучение основ дискретно-событийного моделирования телекоммуникационных 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 инфокоммуникационных сетей и систем
Раздел 2. Работа с пакетом моделирования Riverbed Modeler
Введение. Создание топологии сети. Редактирование атрибутов объектов. Сбор статистики. Настройка параметров моделирования. Просмотр и анализ результатов. Генерация трафика. Настройка профилей пользователей
Раздел 3. Работа с пакетом моделирования ns-2
Введение. Создание топологии сети. Генерация трафика. Сбор статистики. Просмотр и анализ результатов
Раздел 4. Работа с пакетом моделирования QualNet
Введение. Создание топологии сети. Генерация трафика. Сбор статистики. Просмотр и анализ результатов

Раздел 5. Обработка результатов измерений
Виды измерений. Погрешности. Обработка результатов измерений. Погрешность косвенного измерения

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.
Основные термины и определения в области метрологии и обеспечения единства измерений.
Раздел 2. Теоретические основы метрологии.
Физические величины. Система СИ. Измерительные шкалы. Классификация измерений. Теория подобия. Постулаты теории измерений
Раздел 3. Погрешности измерений и неопределенности результатов измерени
Классификация погрешностей. Систематические погрешности и методы их исключения. Промахи и методы их исключения. Случайные погрешности и их вероятностное описание. Неопределенности результатов измерений типа А и типа В. Суммирование погрешностей. Погрешности косвенных измерений
Раздел 4. Методы статистической обработки результатов измерени
Однократные измерения. Статистическая обработка многократных измерений. Доверительный интервал и доверительная вероятность. Оценка неопределенности в измерениях. Правила округления результатов измерений и значений погрешности. Методы идентификации формы закона распределения погрешностей. Информационная теория измерений
Раздел 5. Нормируемые метрологические характеристики средств измерений
Классификация средств измерений. Метрологические характеристики средств измерений, классы точности. Методы измерений. Эталоны единиц электрических величин
Раздел 6. Обеспечение единства измерений Закон РФ «Об обеспечении единства измерений». Государственное регулирование в области обеспечения единства измерений. Формы государственного регулирования в области обеспечения единства измерени
Утверждение типа стандартных образцов или средств измерений. Поверка средств измерений. Калибровка средств измерений
Раздел 7. Метрологическая экспертиза
Закон РФ «Об обеспечении единства измерений». Государственное регулирование в области обеспечения единства измерений. Формы государственного регулирования в области обеспечения единства измерений
Раздел 8. Порядок подтверждения метрологической пригодности средств измерений
Объекты метрологической экспертизы. Обязательная и добровольная метрологические экспертизы. Порядок проведения обязательной метрологической экспертизы
Раздел 9. Аккредитация в области обеспечения единства измерений
Цели аккредитации в области обеспечения единства измерений. Принципы аккредитации. Положение о системе аккредитации в области обеспечения единства измерений.

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:
Целью преподавания дисциплины является изучение сферы своей будущей деятельности, подготовка к выбору профиля своего дальнейшего обучения

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. Профессор М.А.Бонч-Бруевич. СПбГУТ. Факультет ИКСС. Кафедра ЗСС
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. Структура направления подготовки
ФГОС, назначение, структура документа. Рассмотрение учебного плана подготовки по направлению информационная безопасность
Раздел 3. Криптография в истории. От древнего мира до II мировой войны.
История критографии. Первые шифры. Библейский шифр, шифры Цезаря, Виженера,

трафоретная система шифрования, шифры первой Отечественной войны, шифры первой мировой войны, Энигма.
Раздел 4. Криптография в России и СССР
История криптографии в России и СССР.
Раздел 5. История телекоммуникаций и компьютерных сетей
Истрия связи, компьютерные сети, возникновение Internet.
Раздел 6. Хакеры и проблемы информационной безопасности
Феномен хакеров, причины появления, примеры. Актуальность вопросов информационной безопасности в современном мире.
Раздел 7. Информационная война и промышленный шпионаж в современном мире
Информационная война, исторические примеры, примеры из текущих новостей. Промышленный шпионаж в современном мире – примеры. 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:

Овладение принципами обеспечения информационной безопасности автоматизированных систем, использующих в своей структуре компоненты сети интернет.

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) «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. Защищенные протоколы
Виртуальные частные сети. Задачи, решаемые VPN. Туннелирование в VPN. Уровни защищенных каналов.
Раздел 2. Интернет-технологии
Архитектура web-сервера. Модель «клиент-сервер». Модель сервера приложений. Трехуровневая архитектура. Взаимодействие компонентов.
Раздел 3. SQL-инъекции
Принцип внедрения SQL-кода в приложении. Особенности языка SQL для реализации инъекций. Уязвимости, используемые при SQL-инъекциях
Раздел 4. Аутентификация на web-сервере
Средства идентификации и аутентификации, методы разделения ресурсов, технологии разграничения доступа.
Раздел 5. Обеспечение доступности web-приложения
Сервис высокой доступности (HA). Кластерная организация web-ресурсов

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:

дисциплины является получение фундаментальных знаний в области организации локальных вычислительных сетей. Рассматриваются модели взаимодействия сетевых устройств. Изучаются основные протоколы ЛВС(Ethernet, IPv4, IPv6, TCP, UDP и др.)

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) «Безопасность беспроводных локальных сетей».

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. Введение в коммутируемые сети
Дизайн локальных вычислительных сетей. Конвергированные сети. Сети без границ. Уровни построения сети (ядра, распределения, доступа). Коммутируемые сети. Методы обработки кадров. Понятие коллизионных доменов.
Раздел 2. Основы коммутации
Запуск коммутатора. Запуск коммутатора. Конфигурирование портов коммутатора. Режимы дуплекса. Поиск неисправностей на уровне доступа. Удаленный доступ к коммутатору. Протокол SSH. Аспекты защиты в коммутируемых сетях (MAC address flooding, dhcp spoofing). Рекомендации по организации защиты информации в коммутируемых сетях. Функция port-security.
Раздел 3. Виртуальные локальные сети (VLAN)
Сегментация VLAN. Типы VLAN, голосовые VLAN. Понятие транка. Стандарт 802.1q. Тэгирование Ethernet. Настройка VLAN на коммутаторах. Конфигурирование транковых портов. Динамический протокол инициализации транка (DTP). Поиск неисправностей при использовании VLAN. Рекомендации по дизайну VLAN.
Раздел 4. Маршрутизация между VLAN
Организация маршрутизации между VLAN. Модели Router-on-a-Stick и многоуровневой коммутации. Конфигурация маршрутизации между VLAN. Поиск неисправностей в маршрутизации между VLAN.
Раздел 5. Настройка протокола OPSFдля одной области
Протокол OSPF. Компоненты OSPF. Установка сессии. Hello-протокол. Обновления LSA. Принципы работы протокола OSPF. Понятие DR и BDR маршрутизаторов. Идентификатор маршрутизатора. Использование loopback-интерфейсов. Настройка протокола OSPF на интерфейсах. Инверсная маска. Понятие пассивного интерфейса. Метрика протокола OSPF. Полоса пропускания. Настройка протокола OSPF для одной области. Сравнение

протоколов OSPFv2 и OSPFv3. Настройка протокола OSPFv3 для IPv6.
Раздел 6. Листы контроля доступа (ACL)
Назначение листов контроля доступа. Фильтрация пакетов. Типы листов контроля доступа: стандартные и расширенные. Способы настройки ACL: нумерованные, именованные. Инверсная маска. Правила расчета инверсной маски. Общие практики создания ACL. Правила назначения листов контроля доступа на интерфейсах. Создание стандартных ACL (нумерованных и именованных). Редактирование листов контроля доступа. Статистика. Проверка конфигурации ACL. Создание расширенных ACL. Проверка ACL. Настройка ACL на виртуальных терминальных линиях. Типичные ошибки при настройке ACL. Создание листов контроля доступа IPv6. Применение ACL на интерфейсах. Проверка ACL для IPv6.
Раздел 7. Протокол DHCP
Протокол DHCPv4. Сообщения DHCP. Настройка протокола DHCP. Поиск неисправностей настройки протокола DHCP. SLAACи протокол DHCPv6. Настройка SLAAC и DHCPv6. Настройка маршрутизатора в качестве stateless DHCP v6 сервера. Настройка маршрутизатора в качестве stateful клиента. Поиск неисправностей протокола DHCP.

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 AstraLinux» 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) «Защита в

операционных системах».

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 ОС Linux
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. Основы взаимодействия с ОС AstraLinux.
Установка и настройка ОС. Системные компоненты: управления устройствами, файловой системой, пользователями, перезагрузка и отключение. Системные сервисы и команды: сервисы, командный и графический интерфейс. Базовые сетевые службы.
Раздел 3. Средства организации единого пространства пользователей.
Единое пространство пользователей (ЕПП) – средства организации пользователей 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 4. Управление программными пакетами и резервирование.
Установка и удаление программ. Набор команд dpkg. Комплекса программ apt. Обновление программ и системы. Виды резервного копирования. Планирования резервного копирования. Инфраструктура для управления системой резервного копирования. Утилиты rsync и tar.
Раздел 5. Разграничение доступа в ОС AstraLinux.
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. Мандатное разграничение доступом в СУБД и комплексах программ
Раздел 6. Дополнительные механизмы обеспечение безопасности.
Очистка памяти. Изоляция модулей. Маркировка печатных документов. Защита ввода-вывода информации на внешний носитель. Сопоставление пользователя и устройство. Контроль целостности. Режимы киоска и запрета установки исполняемого бита.
Раздел 7. Аудит системы безопасности и восстановление.

Средства управления протоколированием. Особенности системы протоколирование событий. Регистрация событий в СУБД. Восстановление после сбоев и отказов.

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:
Целью изучения 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) «Введение в профессию».

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

<u>Раздел 1. Методы экспериментов с черным ящиком</u>
Методы экспериментов с черным ящиком; Статический метод; Динамический метод.

Раздел 2. Методы исследования программ
Метод маяков; Метод Step-Trace первого этапа; Метод аппаратной точки останова; Динамическое изменение кода программы; Искусственное усложнение структуры программы; Нестандартное обращение к функциям операционной системы; Искусственное усложнение алгоритмов обработки данных; Выявление фактов выполнения программы под отладчиком.
Раздел 3. Особенности анализа программ
Особенности анализа оверлейновых программ; Особенности анализа графических программ; Особенности анализа параллельного кода; Особенности анализа кода в режиме ядра Windows.
Раздел 4. Защита программ от анализа
Динамический метод; Искусственное усложнение структуры программы; Искусственное усложнение структуры программы; Искусственное усложнение алгоритмов обработки данных; Выявление факта выполнения программы под отладчиком.
Раздел 5. Модели взаимодействия программной закладки с атакуемой системой
Модель «наблюдатель»; Модель «перехват»; Модель «искажение»; Несанкционированное использование средств динамического изменения полномочий; Порождение дочернего процесса системным процессом; Модификация машинного кода монитора безопасности.
Раздел 6. Предпосылки к внедрению программ закладок
Модель «наблюдатель»; Модель «перехват»; Модель «искажение»; Несанкционированное использование средств динамического изменения полномочий; Порождение дочернего процесса системным процессом; Модификация машинного кода монитора безопасности.
Раздел 7. Методы внедрения программных закладок
0Классификация методов внедрения программных закладок; Маскировка программной закладки под прикладное программное обеспечение; •Маскировка программной закладки под системное программное обеспечение; •Подмена системного программного обеспечения; •Прямое ассоциирование; •Косвенное ассоциирование.
Раздел 8. Защитные механизмы
Методы защиты; Классификация защит по роду секретного ключа; Надежность защиты; Недостатки готовых "коробочных" решений.
Раздел 9. Распространенные ошибки реализации защитных механизмов
Защита от несанкционированного копирования и распространения серийных номеров; Защита испытательным сроком и ее слабые места; Проблема переустановки; Реконструкция алгоритма; Несколько серийных номеров в одном; Регистрационные данные в памяти; Когда и криптография не спасает; Константы, говорящие сами за себя.

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:

изучение основных концепций организации глобальных вычислительных сетей, принципов адресации, контроля доступа, научиться настраивать основные протоколы канального уровня (HDLC, PPP, Frame Relay), искать неисправности в глобальных вычислительных 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».

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. Иерархический сетевой дизайн
Иерархический дизайн сетей. Архитектура CiscoEnterprise. Модуль сети кампуса, границы сети. Архитектура сетей без границ, средств совместной работы, дата-центов и виртуализации.
Раздел 2. Глобальные сети
Методы доступа к устройствам через глобальную сеть Интернет. Терминология глобальных сетей. Коммутация каналов. Коммутация пакетов. Архитектура сетей сервис-провайдеров. Инфраструктура частных сетей: выделенные линии, dial-up, ISDN, FrameRelay, ATM, EthernetMAN, MPLS, VSAT. Инфраструктура публичных сетей: DSL,

Cable, Wireless, 3G/4GCellular, VPN.
Раздел 3. Соединения вида точка-точка
Серийные и параллельные соединения. Временное разделение каналов. Виды серийных кабелей. DCE/DTE устройства. Инкапсуляция HDLC. Конфигурация HDLC. Протокол PPP. LCP, NCPподуровни. Установка сессий PPP. Аутентификация PPP. Поиск неисправностей в глобальных сетях с использованием протоколов HDLC, PPP.
Раздел 4. Протокол Frame Relay
Преимущества использования протокола Frame Relay. Виртуальные каналы. Инкапсуляция Frame Relay. LMI. Понятие адресации DLCI. Методы обеспечения качества обслуживания Frame Relay. Point-to-point, multipoint сабинтерфейсы. Поиск неисправностей в сетях Frame Relay.
Раздел 5. Сетевая трансляция адресов ipv4 (NAT)
Терминология NAT. Статическая, динамическая трансляция сетевых адресов. Трансляция портов. Преимущества и недостатки NAT. Проверка функционирования NAT. Конфигурация NAT. Анализ таблиц трансляции. Потребности NAT для ipv6.
Раздел 6. Решения для широкополосного доступа
Удаленная работа Teleworking. DSL/ADSL. Типы беспроводных глобальных соединений. Сравнение технологий обеспечения широкополосного доступа. PPPoE.
Раздел 7. Организация безопасных Site-to-site тунней.
Основы VPN. Преимущества VPN. Виды VPN: Site-to-site, remote-access. GRE- туннели. Стек протоколов IPSec. Протокол SSL/TLS.
Раздел 8. Мониторинг сети
Работа протокола Syslog. Конфигурирование Syslog. Работа протокола SNMP. Работа протокола NetFlow. Работа с NetFlow-коллектором.
Раздел 9. Поиск неисправностей в сетях
Документация сети. Аудит. Поиск неисправностей в современных сетях. Сбор информации о сети. Поиск неисправностей в сетях. Поиск неисправностей в IP-сетях.

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:

Является ознакомление слушателей с основными возможностями языка программирования Ассемблер. Особое внимание уделяется изучению вопросам низкоуровнего программирования, понятию организации современного компьютера.

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) «Введение в профессию».

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. Организация современного компьютера
Машинный язык и язык ассемблера. История процессоров Intel.
Раздел 2. Синтаксис ассемблера
Синтаксис ассемблера (Операнды, Операнды-выражения). Директивы сегментации. Простые типы данных.
Раздел 3. Сложные структуры данных
Массивы (Описание и инициализация массива, доступ к элементам, двухмерные массивы, типовые операции), структуры (Описание структуры, определение данных с типом структуры, методы работы со структурой),объединения.
Раздел 4. Команды ассемблера
Команды обмена данных, арифметические команды, логические команды и команды сдвига, команды передачи управления, цепочечные команды.
Раздел 5. Программирование типовых управляющих структур
Условный оператор, операторы цикла, функции
Раздел 6. Защита от копирования
Классификация методов защиты информации, Стохастическое преобразование информации, Особенности программной реализации алгоритмов защиты информации
Раздел 7. 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

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 вредоносного программного обеспечения
Основные понятия и определения, Инструментарий для создания вредоносных программ. Стиль «опасного» программирования, Состав вредоносных программ и команд
Раздел 2. Антивирусные программы
Классификация антивирусных программ, Уровни защиты от компьютерных вирусов, Защита от деструктивных действий и размножения вирусов
Раздел 3. Функциональные виды вредоносных программ
Вредоносные программы «удаленного администрирования», Сетевые черви, Троянцы и другие различные виды
Раздел 4. Способы внедрения вредоносных программ
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
Внедрение и запуск на этапе самотестирования компьютера, Внедрение и запуск опасных программ с помощью «троянских» оболочек, Внедрение и запуск опасных команд с использованием ярлыков

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) «Защита в операционных системах».

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: изучение студентами особенностей применения стеганографии и предъявляемых к ней требования. Дисциплина «Основы стеганографии» должна обеспечивать формирование фундамента подготовки будущих специалистов в области защиты авторских прав, обеспечения целостности передаваемой или сохраняемой информации на носителях с помощью стеганографических методов защиты информации, а также, создавать необходимую базу для успешного овладения последующими специальными дисциплинами учебного плана.

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) «Криптографические протоколы».

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:

Целью преподавания дисциплины является изучение принципов организации защиты информации в центрах обработки данных. Дисциплина «Защита информации в центрах обработки данных» должна обеспечивать формирование фундамента подготовки будущих специалистов в области защиты информации, а также, создавать необходимую базу для успешного овладения последующими специальными дисциплинами учебного плана.

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) «Защита информации с помощью маршрутизаторов и коммутаторов».

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. Настройка механизмов защиты виртуальных сетей
Private VLAN, фильтрация по MAC-адресам, traffic policing и traffic shaping.

Раздел 4. Настройка прав доступа к ЦОД
AAA протокол, разграничение прав доступа пользователей.
Раздел 5. Настройка защиты виртуального хранилища
SAN зоны, Virtual SAN, шифрование данных, защита данных, обеспечение безопасности iSCSI.
Раздел 6. Работа с ресурсами, мониторинг ресурсов
Работа с виртуальными ресурсами, распределение ресурсов, мониторинг и управление ресурсами ЦОД
Раздел 7. Механизмы высокой доступности (HA)
Внедрение технологий избыточности в ЦОД, принципов отказоустойчивости, механизмов резервного копирования данных
Раздел 8. Дизайн ЦОД
Принципы построения центров обработки данных, примеры современных решений на рынке.

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:

формирование фундамента подготовки будущих специалистов в области теории построения сетей, кибернетики, 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 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) «Защита информации в центрах обработки 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
Рассматривается 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. Рассматриваются 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)
Рассматриваются все современные методы создания VPN, включая такие методы, как: IPsecVTI, динамические VTI, GETVPN, DMVPN, FlexVPN. Рассматриваются структуры протоколов IPsec, IKEv.1 иv.2, приведены сравнительные характеристики всех современных методов построения VPN. Рассматриваются протоколы построения шифрованных туннелей трафика SSL/TLS. Приводятся основные уязвимости протоколов и способы борьбы с ними.
Раздел 7. Защита контроллера SDN
Рассматриваются принципы организации защиты SDN контроллера, на примере компании Cisco Systems.
Раздел 8. Системы детекции/предотвращения вторжений и аномалий
Рассматриваются системы предотвращения вторжений и аномалий (на примере ПО с открытым исходным кодом – Snort)
Раздел 9. Защита OpenStack

Рассматривается 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

Приводятся конфигурации и принцип действия фаерволов следующего поколения (NGFW)

Раздел 11. Конфиденциальность облачных вычислений. Целостность облачных вычислений

Приводятся основные угрозы и стратегии защиты облачных вычислений.
Рассматриваются основные угрозы целостности данных и методы защиты от угроз в облачных вычислениях.

Раздел 12. Доступность облачных вычислений. Учет облачных вычислений. Сохранность данных в облаке.

Основные угрозы доступности облачных вычислений, средства для устранения угроз, стратегии защиты. Шифрование данных в облаке, методы защиты и обеспечения сохранности данных в облаке.

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 Допуск должностных лиц, работников к конфиденциальной информации 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

<u>Раздел 1. История развития операционных систем</u>
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:

изучение студентами способов сертификации средств защиты информации.

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:
изучение студентами способов сертификации средств защиты информации.

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. 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, пр

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:
студентами сущности, содержания и особенностей технологий обеспечения информационной безопасности для больших данных (Big Data)

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) «Защита в операционных системах».

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. Введение
Цели и задачи освоения дисциплины. Содержание дисциплины. Принципы и методы изучения дисциплины.
Раздел 2. Большие данные (Big Data)
Основные механизмы работы Big Data, принципиальные отличия от классических систем управления базами данных (СУБД).
Раздел 3. Принципы организационного проектирования систем Big Data.
Рассмотрение основных моделей обработки больших данных, основных наиболее распространенных решений в сфере информационной безопасности на основе Big Data.
Раздел 4. Работа с Big Data
Рассмотрение стандартных механизмов сбора и анализа неструктурированной информации, а также обработка полученных данных из этой информации.

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:

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 «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».

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
Основные типы атак, примеры атак, архитектура x86,
Раздел 3. Фишинговые атаки, угрозы онлайн банкинга
Определение и классификация фишинтовых атак, детекция атак, обзор угроз онлайн банкинга, примеры атак, методы защиты
Раздел 4. Программное обеспечение, предназначенное для вымогательства
КлассификацияугрозRansomwareandScareware. 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
ОбзорWindowsKernel (ядраОСWindows), понятие руткитов, эволюция руткитов. Понятие буткитов, эволюция.
Раздел 10. Антивирусные технологии
Определение комплексныхактивирусов, 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:
LДисциплина должна обеспечивать 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, обзорфункций 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:

изучение принципов работы межсетевых экранов и систем предотвращения вторжений и аномалий.

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».

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 базового контроля доступа Тонкая настройка базовых функций инспектирования, основанного на состоянии сессии Настройка продвинутых функций контроля доступа
Раздел 4. Внедрение функций по виртуализации и обеспечению высокой доступности

Внедрение трансляции сетевых адресов Настройка прозрачного режима
Раздел 5. Выполнять первоначальную настройку сенсора IPS
Принципы работы сенсоров. Сигнатуры, настройка сигнатур, ложное срабатывание.
Раздел 6. Выполнять оптимизацию политик сенсора для корректного реагирования в рамках конкретной сети
Тонкая настройка политик работы сенсора для корректного реагирования, конфигурирование синатур.

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 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

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:
изучение методов анализа угроз корпоративной сети

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:

Целью преподавания дисциплины является изучение механизмов и способов построения доверенной среды передачи на основе виртуальных частных соединений. Дисциплина «Построение доверенной среды передачи» должна обеспечивать формирование фундамента подготовки будущих специалистов в области защиты инфокоммуникационых сетей и систем, а также, создавать необходимую базу для успешного овладения последующими специальными дисциплинами учебного плана

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 в операционных системах»; «Криптографические протоколы».

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. Технологии VPN
Анализ уязвимости протоколов построения VPN
Раздел 2. Инфраструктура открытых ключей (PKI)
Использование инфраструктуры открытых ключей (PKI)
Раздел 3. VPN на основе протоколов IPsec ч.1
Построение модели виртуальной частной сети типа «Объединение удаленных площадок» на основе стека протоколов IPsec
Раздел 4. VPN на основе протоколов IPsec ч.2
Построение модели виртуальной частной чети типа «удаленного доступа» на основе стека протоколов IPsec
Раздел 5. VPN на основе протоколов SSL/TLS
Построение модели виртуальной частной чети типа «удаленного доступа» на основе протоколов SSL/TLS
Раздел 6. Методы аутентификации и авторизации для контроля доступа пользователей к ресурсам VPN
Использование расширенных методов аутентификации и авторизации для контроля доступа пользователей к ресурсам VPN

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:
изучение архитектуры,структуры,функции,компонентов беспроводных локальных 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».

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 IEEE 802.11
IEEE 802.11 — набор стандартов связи для коммуникации в беспроводной локальной сетевой зоне частотных диапазонов 0,9, 2,4, 3,6 и 5 ГГц.
Раздел 2. Основные принципы радиоанализа и радиопланирования
Принципы распределения радиоволн, виды антенн, расчет допустимой мощности.
Раздел 3. Основы и принципы работы протокола RADIUS, DIAMETER, семейство протоколов EAP
Протоколы RADIUS, DIAMETER, семейство протоколов EAP.
Раздел 4. Стандарт IEEE 802.1x, технологии профилирования в беспроводных сетях стандарта IEEE 802.11
IEEE 802.1x – стандарт аутентификации пользователей в сети.
Раздел 5. Технологии динамического изменения авторизации
Настройка динамического изменения авторизации
Раздел 6. Администрирование интерфейса конечных пользователей
Администрирование интерфейса конечных пользователей в системе Cisco UC
Раздел 7. Возможности телефонии и мобильности, и поддержка решения Cisco UC
Настройка возможностей телефонии и мобильности, поддержка решения Cisco UC

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:

изучение основных проблем, возникающих при разработке приложений для мобильных устройств, а также получение представления о проблемах, стоящих перед разработчиком таких 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 «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 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. Обзор мобильных платформ
Обзор мобильных платформ
Раздел 2. Работа с приложениями
Создание приложений. Реализация интерфейсов. Управление ресурсами. Хранение информации. Доступ с аппаратным возможностям
Раздел 3. Изучение структуры защищенных мобильных приложений
Просмотр исходного кода, постановка требований на доработку. Дополнительные задания

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. Знакомство с протоколами, обеспечивающими передачу данных в реальном времени – RTP, RTCP и сигнализационными протоколами SIP, MGCP, H.323

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 «Безопасность беспроводных локальных сетей».

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
Предмет и основные задачи дисциплины «Безопасность IP-телефонии», её значение в сис¬теме подготовке бакалавров по направлению «Инфокоммуникационные технологии и системы связи»
Раздел 2. Кодеки, используемые в IP-телефонии. Цифровой сигнальный процессор (DSP).
Классификация VoIP кодеков. Типы цифровых сигнальных процессоров. Расчет требуемой полосы пропуская в зависимости от вида кодека. Настройка DSP.
Раздел 3. Сигнализация в VoIPсетях. Рекомендации H.323. Протоколы SIP и SDP
Протоколысигнализации H.323, Session Initiation Protocol (SIP), MGCP протокол. Стадии обработки голосового трафика. Компоненты VoIP. Квантование. Сэмблирование.
Раздел 4. Особенности передачи голоса в IP-сетях. Протокол RTP.
Сравнение традиционной телефонной сети общего пользования и VoIP. Протоколы RTP и

RTCP. Формат кадра RTP протокола. Установление VoIP-сессии.
Раздел 5. Механизмы обеспечения QoS для VoIP.
Обзор моделей качества обслуживания (QoS): дифференцированного обслуживания (DiffServ), интегрированного сервиса (IntServ), негарантированная доставки (BestEffort). Механизмы обеспечения качества обслуживания в сетях передачи голоса: маркировка, приоретизация, полисинг, шейпинг трафика. CiscoAutoQoS.
Раздел 6. Введение в CUCM Express.
Настройка CUCM Express на маршрутизаторе Cisco, функции CUCM Express в голосовой среде.
Раздел 7. Пограничные контроллеры сессий (SBC).
Механизмы защиты голосового трафика: конфиденциальность, целостность, аутентификация. Протокол Secure RTP. Алгоритмы шифрования: DES, 3DES, AES. Защита от распределенных атак обслуживания (DDoS).

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:

Целью преподавания дисциплины является изучение архитектуры, настройки IP-телефонии. Кроме того, студенты знакомятся с протоколами, обеспечивающими передачу данных в реальном времени – RTP, RTCP и сигнализационными протоколами SIP, MGCP, H.323.

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 «Защита операционных систем сетевых устройств».

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
Предмет и основные задачи дисциплины «Защита голосового трафика в сети Интернет», её значение в системе подготовке бакалавров по направлению «Инфокоммуникационные технологии и системы связи».
Раздел 2. Кодеки, используемые в IP-телефонии. Цифровой сигнальный процессор (DSP).
Классификация VoIP кодеков. Типы цифровых сигнальных процессоров. Расчет требуемой полосы пропуская в зависимости от вида кодека. Настройка DSP
Раздел 3. Сигнализация в VoIPсетях. Рекомендации H.323. Протоколы SIP и SDP.
Протоколысигнализации H.323, Session Initiation Protocol (SIP), MGCP протокол. Стадии обработки голосового трафика. Компоненты VoIP. Квантование. Сэмблирование.
Раздел 4. Особенности передачи голоса в IP-сетях. Протокол RTP.
Сравнение традиционной телефонной сети общего пользования и VoIP. Протоколы RTP и RTCP. Формат кадра RTP протокола. Установление VoIP-сессии.
Раздел 5. Механизмы обеспечения QoS для VoIP.
Обзор моделей качества обслуживания (QoS): дифференцированного обслуживания (DiffServ), интегрированного сервиса (IntServ), негарантированная доставки (BestEffort). Механизмы обеспечения качества обслуживания в сетях передачи голоса: маркировка, приоретизация, полисинг, шейпинг трафика. CiscoAutoQoS.
Раздел 6. Введение в CUCM Express.
Настройка CUCM Express на маршрутизаторе Cisco, функции CUCM Express в голосовой среде.
Раздел 7. Пограничные контроллеры сессий (SBC).
Механизмы защиты голосового трафика: конфиденциальность, целостность, аутентификация. Протокол Secure RTP. Алгоритмы шифрования: DES, 3DES, AES. Защита от распределенных атак обслуживания (DDoS).

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

Б1.В.ДВ.03.01 Блокчейн и эллиптическая криптография

Цели освоения дисциплины

Целью преподавания дисциплины «Блокчейн и эллиптическая криптография» является:

Изучение технологии блокчейн, а также вопросов и основ эллиптической криптографии. Дисциплина "Блокчейн и эллиптическая криптограия" должна обеспечивать формирование фундамента подготовки будущих специалистов в области криптозащиты и блокчейна, а также, создавать необходимую базу для успешного изучения в областях криптографии.

Место дисциплины в структуре ОП

Дисциплина «Блокчейн и эллиптическая криптография» 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».

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 криптографии. Понятие технологии блокчейн. Основные сферы применения блокчейна. Связь криптографии и блокчейна
Раздел 2. Элементы теории эллиптических кривых над конечными полями
Задача Диффи-Хеллмана. Криптосистема Эль-Гамаля. Понятие эллиптической кривой. Теорема Хассе. Понятие конечной группы . Определение операции нахождения противоположного элемента и суммы элементов на эллиптической кривой
Раздел 3. Задание КС над эллиптическими кривыми
Тестирование простых чисел. Факторизация больших чисел. Вычисления дискретных логарифмов. Построения новых криптосистем с ОК. Построения новых систем с цифровыми подписями
Раздел 4. Обобщение КС Эль-Гамаля на случай эллиптических кривых

Генерирование ключей. Шифрование. Дешифрование
Раздел 5. Построение системы распределения ключей Диффи-Хеллмана над эллиптическими кривыми
Согласование эллиптической кривой над полем. Согласование точки на кривой. Стойкость метода распределения ключей
Раздел 6. Проблематика и вопросы Блокчейна
Ethereum. Публичный ключ, частный ключ. Разница между Ethereum и биткойн-блокчейном. Компоненты экосистемы блокчейна. Блоки в технологии блокчейн

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:

Целью преподавания дисциплины является изучение вопросов основ криптографической защиты 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 «Введение в профессию».

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. Математический базис криптосистем с открытым ключе
Введение в курс. Основные понятия и определения. Модульная арифметика. Теорема Ферма. Теорема Эйлера. Факторизация, возведение в степень логарифмирование Конечные поля, способы представления. Оценки сложности вычислений. Квадратичные вычеты и тестирование простых чисел.
Раздел 2. Системы шифрования с открытыми кючами
Криптосистемы Эль-Гамаля, РША, Рабина, Мас-Элис. Генерирование ключей, шифрование, дешифрование. Атаки на криптосистемы.
Раздел 3. Системы электронной цифровой подписи
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 4. Криптографические протоколы
Обзор основных протоколов. Изучение протоколов разделения секрета, аутентификация пользователей с нулевым разглашением, секретные совместные вычисления, тайное голосование.
Раздел 5. Управление открытыми ключами
Принцип построения инфраструктуры открытых ключей (PKI), назначение и использование сертификатов открытых 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:

изучение вопросов защиты операционных систем. Дисциплина «Защита операционных систем сетевых устройств»должна обеспечивать формирование фундамента подготовки будущих специалистов в области системного ПО, а также, создавать необходимую базу для успешного овладения последующими специальными дисциплинами учебного плана.

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 «Безопасность беспроводных локальных сетей»; «Защита в операционных системах».

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. История развития операционных систем
История разработки ОС MSDOS, WindowsиUnix.Версии ОС. Стандарт POSIX. Развитие проекта GNU, лицензия GNUGPL. Создание и развития дистрибутивовGNU/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.
Раздел 3. Основы управление доступом в ОС GNULinux.
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.

Раздел 4. Управление безопасностью SELinux
Организация и мониторинг Security-EnhancedLinux. Управление моделью безопасности SELinux: моды, контексты. Описание прав доступа к файлам и процессам.
Раздел 5. Контроль сетевого трафика в ОС GNULinux.
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.
Раздел 6. 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.
Раздел 7. Роли ОС MSWindowsServer. Реализация доменных служб ActiveDirectory.
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 8. 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 9. Реализация системы безопасности сети в ОС MSWindows.
Утилиты по настройке сети. Угрозы сетевой безопасности, реализация брандмауэров. Настройка брандмауэра Windows. Защита доступа к сети.
Раздел 10. Внедрение программ обеспечения безопасности в ОС MSWindows.
Установка дополнительной системы защиты информации, для упрощения управлением доступом к файлам, на примере системы SearchInform.

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:
изучение студентами принципов построения безопасных

инфокоммуникационных систем и сетей, обеспечение и внедрение средств защиты сетевой инфраструктуры на базе коммутаторов и маршрутизаторов, безопасное подключение филиалов корпоративной сети с помощью виртуальных частных сетей на базе IPsec, поддержка технологии обеспечения удалённого доступа (SSL VPN, Easy VPN) с помощью маршрутизаторов.

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 маршрутизации в компьютерных сетях».

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 SourceGuard. Протокол 802.1x и его компоненты. Протокол EAP, виды аутентификации пользователей посредством протокола EAP.
Раздел 3. 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 4. Внедрение межсетевого экрана на основе зон и политик.
Установка и настройка межсетевого экрана (Zone-basedpolicyfirewall) 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 5. 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 6. 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 7. 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 CiscoEasy VPN. Дизайн, поиск и устранение неисправностей в сетях удаленного доступа.

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.08.01 является дисциплиной по выбору вариативной 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. Методика проведения учебно-тренировочного занятия.
Оценка двигательной активности и суточных энергетических затрат. Базовый комплекс упражнений общей физической подготовки. Использование подвижных, спортивных игр.
Раздел 2. Овладение двигательными навыками и методами проведения занятий по общей физической подготовки.
Методика самооценки уровня и динамики общей и специальной физической подготовленности. Ознакомление и обучение двигательным навыкам на занятиях общей физической подготовки. Базовый комплекс упражнений общей физической подготовки.
Раздел 3. Повышение уровня функциональных и двигательных способностей, направленного формирования качеств и свойств личности.
Методы самоконтроля здоровья, физического развития и функциональной подготовленности. Комплексное занятие: упражнения для развития гибкости, выносливости, силы, быстроты и ловкости. Использование подвижных, спортивных игр.
Раздел 4. Овладение методами и способами физкультурно-спортивной деятельности.
Средства и методы мышечной релаксации в спорте. Методы спортивной тренировки. Комплексное занятие: упражнения для развития основных физических качеств.
Раздел 5. Направленное развитие основных физических качеств. Подготовка к сдаче нормативов ГТО.
Методики самостоятельного освоения отдельных элементов профессионально-прикладной физической подготовки (ППФП). Комплексное занятие: упражнения для развития основных физических качеств. Подготовка к выполнению тестовых испытаний и сдаче нормативов ГТО.
Раздел 6. Приобретение опыта практической деятельности, повышения уровня функциональных и двигательных способностей.
Комплексное занятие: упражнения для развития основных физических качеств. Использование подвижных, спортивных игр.

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.08.02 является дисциплиной по выбору вариативной 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. Методика проведения учебно-тренировочного занятия.
Оценка двигательной активности и суточных энергетических затрат. Базовый комплекс упражнений общей физической подготовки. Использование подвижных, спортивных игр (по упрощенным правилам).
Раздел 2. Овладение двигательными навыками и методами проведения занятий по общей физической подготовке.
Методика самооценки уровня и динамики общей и специальной физической подготовленности. Ознакомление и обучение двигательным навыкам, на занятиях общей физической подготовки. Базовый комплекс упражнений общей физической подготовки.
Раздел 3. Повышение уровня функциональных и двигательных способностей, направленного формирования качеств и свойств личности.
Методы самоконтроля здоровья, физического развития и функциональной подготовленности. Комплексное занятие: упражнения для развития гибкости, выносливости (адаптивные формы), силы (адаптивные формы), быстроты и ловкости.

Использование подвижных, спортивных игр (по упрощенным правилам).
Раздел 4. Овладение методами и способами физкультурно-спортивной деятельности.
Средства и методы мышечной релаксации в спорте. Методы спортивной тренировки. Комплексное занятие: упражнения для развития основных физических качеств (адаптивные формы).
Раздел 5. Развитие физических качеств и совершенствование координационных способностей.
Методики самостоятельного освоения отдельных элементов профессионально-прикладной физической подготовки. Комплексное занятие: упражнения для развития основных физических качеств (адаптивные формы). Использование подвижных, спортивных игр (адаптивные формы). Подготовка к выполнению тестовых испытаний, доступных по медицинским показаниям.
Раздел 6. Приобретение опыта практической деятельности, повышение уровня функциональных и двигательных способностей.
Комплексное занятие: упражнения для развития основных физических качеств (адаптивные формы). Использование подвижных, спортивных игр (по упрощенным правилам).

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.08.03 является дисциплиной по выбору вариативной 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. Методика проведения учебно-тренировочного занятия.
Оценка двигательной активности и суточных энергетических затрат. Комплексное занятие: упражнения для развития гибкости, выносливости, силы, быстроты и ловкости.
Раздел 2. Овладение двигательными навыками, техническими приемами, индивидуальной и групповой тактики в избранном виде спорта.
Методика самооценки уровня и динамики общей и специальной физической подготовленности по избранному виду спорта или системе физических упражнений. Ознакомление и обучение двигательным навыкам, техническими приемами в избранном виде спорта. Комплексное занятие: упражнения для развития основных физических качеств. Использование подвижных, спортивных игр.
Раздел 3. Повышение уровня функциональных и двигательных способностей, направленного формирования качеств и свойств личности.
Методы самоконтроля здоровья, физического развития и функциональной подготовленности. Комплексное занятие: упражнения для развития гибкости, выносливости, силы, быстроты и ловкости. Использование подвижных, спортивных игр.
Раздел 4. Овладение методами и способами физкультурно-спортивной деятельности.
Средства и методы мышечной релаксации в спорте. Методы спортивной тренировки. Комплексное занятие: Упражнения для развития основных физических качеств в избранном виде спорта.
Раздел 5. Направленное развитие основных физических качеств и совершенствование координационных способностей.
Методики самостоятельного освоения отдельных элементов профессионально-прикладной физической подготовки. Комплексное занятие: упражнения для развития основных физических качеств в избранном виде спорта (Гиревой спорт, Атлетическая гимнастика, Спортивные игры, Гребной спорт).
Раздел 6. Приобретение опыта практической деятельности, повышения уровня функциональных и двигательных способностей.
Практика проведения соревнований по различным видам спорта. Занятия различными видами 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:
изучение вопросов лицензирования программного обеспечения в телекоммуникационных системах. Дисциплина «Программы для ЭВМ и базы данных как объекты интеллектуальной собственности» должна обеспечивать формирование фундамента подготовки будущих специалистов в области инфокоммуникаций, а также, создавать необходимую базу для успешного овладения последующими специальными дисциплинами учебного плана.

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».

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. Определение понятия лицензирования ПО
Формулировка понятий лицензирования ПО. Принципы и методы лицензирования ПО.
Раздел 2. Необходимость лицензирования ПО
Значение необходимости лицензирования программного обеспечения
Раздел 3. Классификация лицензий ПО и типы лицензий
Сравнение типов лицензий ПО и определение признаков каждого из типов.
Раздел 4. Тенденция развития лицензирования ПО
Скорость развития лицензирования ПО и рассмотр того с чем это связано
Раздел 5. Практическое применение лицензирования ПО
Где применяется лицензирование ПО и при каких условиях

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) .

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 проводить контроль защищенности акустической речевой информации от утечки по техническим каналам (ПК-14)
– 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