Аннотации рабочих программ дисциплин

образовательной программы высшего образования.

Направление подготовки «10.03.01 Информационная безопасность», направленность / профиль образовательной программы «Безопасность компьютерных систем»

1. Аннотации рабочих программ дисциплин (модулей) базовой части

Б1.Б.01 История

Цели освоения дисциплины

Целью преподавания дисциплины «История» является:
формирование систематизированных знаний об основных закономерностях и особенностях исторического процесса, определение места российской цивилизации в мировом историческом процессе с учетом стремления к объективности в его освещении; формирование гражданской позиции.

Место дисциплины в структуре ОП

Дисциплина «История» Б1.Б.01 является базовой дисциплиной цикла учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность».
Изучение дисциплины «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:

– способностью анализировать основные этапы и закономерности исторического развития России, ее место и роль в современном мире для формирования гражданской позиции и развития патриотизма (ОК-3)

Содержание дисциплины

Раздел 1. Введение в историю.
1.1.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.1.2. 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.).
1. Средневековье как этап всемирной истории. Периодизация и региональная специфика средневековья. 2.2. 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.

3.1. 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.).3.2. 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.

4.1. 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. 4.2. 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.

5.1. Великая российская революция: 1917-1922. Февраль 1917 г. и его итоги. Октябрь 1917 г. Россия в годы Гражданской войны и интервенции. Образование СССР. 5.2. 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. 5.3. 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.Б.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.Б.02 является базовой дисциплиной цикла учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». 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:

– способностью использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности (ОК-9)

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.Б.03 Иностранный язык

Цели освоения дисциплины

Целью преподавания дисциплины «Иностранный язык» является: повышение 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 бакалавриата по направлению «10.03.01 Информационная безопасность». 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:

– способностью к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности (ОК-7)

Содержание дисциплины

Раздел 1. Учебно-познавательная сфера общения
Высшее образование в России и за рубежом. Студенческая жизнь в России и за рубежом. История и традиции моего вуза.
Раздел 2. Социально-культурная сфера общения
Язык как средство межкультурного общения. Мир природы. Охрана окружающей среды. Плюсы и минусы глобализации. Проблемы глобального языка и культуры.
Раздел 3. Профессиональная сфера общения
Информационные технологии.
Раздел 4. Профессиональная сфера общения (продолжение)
Научно-технический прогресс и его достижения в сфере инфокоммуникационных технологий и систем связи. Плюсы и минусы всеобщей информатизации общества.

Общая трудоемкость дисциплины

252 час(ов), 7 ЗЕТ

Форма промежуточной аттестации

Зачет, Экзамен

Б1.Б.04 Защищенный электронный документооборот

Цели освоения дисциплины

Целью преподавания дисциплины «Защищенный электронный документооборот» является:
изучение вопросов основ построения защищенного документооборота.

Место дисциплины в структуре ОП

Дисциплина «Защищенный электронный документооборот» Б1.Б.04 является базовой дисциплиной цикла учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Изучение дисциплины «Защищенный электронный документооборот» основывается на базе знаний, умений и компетенций, полученных студентами в ходе освоения школьных курсов.

Дисциплина «Защищенный электронный документооборот» Б1.Б.04 является одной из дисциплин базовой части учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Информационные технологии».

Требования к результатам освоения

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

– способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7)

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 пр ава. 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 информации".
В рамках раздела изучаются термины и определения, основные понятия рассматриваемые ФЗ № 149 "Об информации, информационных технологиях и о защите информации". Основные положения ФЗ.
Раздел 5. Персональные данные в соответствии с законом РФ "О персональных данных.
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 Active Directory 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 положения DLP систем. Управление индексами и базами данных компонентов DLP-системы на примере DLP «Контур информационной безопасности Searchinform» при помощи средств Searchinform DataCenter. Поиск по перехваченным документам при помощи приложения SearchinformClient
Раздел 10. Основы электронного документооборота, этапы проектирования
В рамках раздела изучаются особенности проектирования и защиты электронного документооборота, основы защиты баз данных, основы защита корпоративного почтового документооборота.

Общая трудоемкость дисциплины

72 час(ов), 2 ЗЕТ

Форма промежуточной аттестации

Зачет

Б1.Б.05 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 базовой дисциплиной цикла учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Изучение дисциплины «Экономика» 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 использовать основы экономических знаний в различных сферах деятельности (ОК-2)

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

72 час(ов), 2 ЗЕТ

Форма промежуточной аттестации

Зачет

Б1.Б.06 Философия

Цели освоения дисциплины

Целью преподавания дисциплины «Философия» является:
Цель изучения дисциплины – 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 части учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». 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:

– способностью использовать основы философских знаний для формирования мировоззренческой позиции (ОК-1)

Содержание дисциплины

Раздел 1. Что есть философия?
Что есть философия?
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
Философия бытия
Раздел 4. Сознание и познание
Сознание и познание
Раздел 5. Научное познание
Научное познание
Раздел 6. Философия человека
Философия человека
Раздел 7. Социальная философия
Понятие общества и его структура Глобальные проблемы и будущее человечества

Общая трудоемкость дисциплины

144 час(ов), 4 ЗЕТ

Форма промежуточной аттестации

Экзамен

Б1.Б.07 Правоведение

Цели освоения дисциплины

Целью преподавания дисциплины «Правоведение» является:
получение студентами базовых знаний по основным отраслям российского права, приобретение знаний об основах теории государства и права, системе права, современных правовых системах

Место дисциплины в структуре ОП

Дисциплина «Правоведение» Б1.Б.07 является базовой дисциплиной цикла учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Изучение дисциплины «Правоведение» 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 использовать основы правовых знаний в различных сферах деятельности (ОК-4)

Содержание дисциплины

Раздел 1. Основы общей теории права.
Государство как основной субъект правотворчества и правоприменения. Зависимость правотворчества и правоприменения от формы государственно-территориального устройства, формы правления и методов реализации политической власти. Понятие права. Субъективное право и юридическая обязанность. Понятие «норма права». Признаки, структура, виды, толкование норм права. Понятие «источник права». Основные виды источников права: правовой обычай, правовая доктрина, судебный прецедент, священные книги, нормативно-правовой договор, нормативно-правовой акт. Нормативно-правовой акт как основной источник права в Российской Федерации, его виды и признаки. Понятие закона. Порядок принятия законов. Виды и иерархия законов. Правило иерархичности.
Раздел 2. Основы конституционного права РФ.
Конституционное право Российской Федерации как ведущая отрасль национального права. Понятие, предмет, метод правового регулирования и источники конституционного права РФ. Юридические свойства Конституции РФ. Понятие и виды конституционных законов. Структура и правовое положение глав Конституции РФ, процедуры внесения поправок и пересмотра Конституции РФ. Основы конституционного строя РФ. Принципы организации государственной власти в РФ. Государственный орган: понятие, виды, сфера компетенции основных органов государственной власти (законодательной, исполнительной, судебной).
Раздел 3. Основы гражданского права РФ.
Основы гражданского права РФ. Понятие, предмет метод правового регулирования гражданского права. Гражданский кодекс РФ: структура и краткая характеристика разделов. Гражданские правоотношения: специфика, виды и особенности субъектов. Объекты гражданских правоотношений: понятие и виды. Физические лица.
Раздел 4. Основы трудового права РФ.
Трудовое право РФ как самостоятельная отрасль права: понятие и сущность. Источники трудового права РФ. Система социального партнерства как базовый элемент системы локального трудового права: суть и формы. Трудовой Кодекс РФ: характеристика и специфика статей.

Общая трудоемкость дисциплины

72 час(ов), 2 ЗЕТ

Форма промежуточной аттестации

Зачет

Б1.Б.08 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.

Место дисциплины в структуре ОП

Дисциплина «Безопасность жизнедеятельности» Б1.Б.08 является базовой дисциплиной цикла учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность».
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:

– способностью применять приемы оказания первой помощи, методы и средства защиты персонала предприятия и населения в условиях чрезвычайных ситуаций, организовать мероприятия по охране труда и технике безопасности (ОПК-6)

Содержание дисциплины

Раздел 1. Введение в дисциплину. Основные понятия и определения
Характерные системы "человек - среда обитания". Производственная, городская, бытовая, природная среда. Взаимодействие человека со средой обитания. Понятия «опасность», «безопасность». Виды опасностей: природные, антропогенные, техногенные. Чрезвычайные ситуации - понятие, основные виды. Понятие техносферы. Критерии и параметры безопасности техносферы.
Раздел 2. Обеспечение комфортных условий жизнедеятельности
Комфортные (оптимальные) условия жизнедеятельности. Климатическая, воздушная, световая, акустическая и психологическая среды, влияние среды на самочувствие, состояние здоровья и работоспособность человека. Психофизиологические и эргономические условия организации и безопасности труда
Раздел 3. Защита человека и среды обитания от вредных и опасных факторов
Понятие вредного и опасного фактора. Классификация вредных и опасных факторов антропогенного и техногенного происхождения. Параметры, характеристики основных

вредных и опасных факторов среды обитания, их источников. Воздействие основных вредных и опасных факторов на человека и их предельно-допустимые уровни. Методы защиты от вредных и опасных факторов. Общая характеристика и классификация защитных средств.
Раздел 4. Чрезвычайные ситуации и методы защиты в условиях их реализации
Классификация чрезвычайных ситуаций и объектов экономики по потенциальной опасности. Фазы развития чрезвычайных ситуаций. Характеристика поражающих факторов чрезвычайных ситуаций природного характера. Техногенные аварии, их особенности и поражающие факторы. Чрезвычайные ситуации мирного и военного времени и их пора-жающие факторы. Виды оружия массового поражения, их особенности и последствия его применения. Терроризм и террористические действия. Методы прогнозирования и оценки обстановки при чрезвычайных ситуациях. Устойчивость функционирования объектов экономики в чрезвычайных ситуациях. Принципы и способы повышения устойчивости функционирования объектов в чрезвычайных ситуациях. Основы организации защиты населения и персонала в мирное и военное время, способы защиты, защитные сооружения, их классификация. Организация эвакуации населения и персонала из зон чрезвычайных ситуаций. Мероприятия по оценке обстановки и обеспечению безопасных условий для оказания первой помощи. Вызов скорой медицинской помощи, других специальных служб. Мероприятия первой медицинской помощи. Передача пострадавшего бригаде скорой медицинской помощи, другим специальным службам. Средства индивидуальной защиты и порядок их использования. Основы организации аварийно-спасательных и других неотложных работ при чрезвычайных ситуациях.
Раздел 5. Правовые основы безопасности жизнедеятельности
Законодательные и нормативно-правовые акты, регулирующих вопросы охраны труда, промышленной безопасности и безопасности в чрезвычайных ситуациях, гражданской обороны. Ответственность за нарушение требований законодательства и нормативных документов. Страхование рисков: страхование ответственности владельцев опасных производственных объектов, социальное страхование Органы государственного управления безопасностью, органы надзора и контроля за безопасностью. Системы РСЧС и гражданской обороны.

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

Б1.Б.09 История связи

Цели освоения дисциплины

Целью преподавания дисциплины «История связи» является:
изучение возникновения и развития мировой и отечественной связи (почты, телеграфа, телефона, радио, телевидения, интернета).

Место дисциплины в структуре ОП

Дисциплина «История связи» Б1.Б.09 является одной из дисциплин базовой части учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». 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:

– способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия (ОК-6)

Содержание дисциплины

Раздел 1. Зарождение средств связи.
Выделение человека из животного мира. Первая информационная революция. Язык как средство связи. Звуковые средства связи. Визуальные средства связи.
Раздел 2. Возникновение и развитие почты.
Переход от присваивающего хозяйства к производящему – формирование аграрных обществ. Появление письменности как вторая информационная революция. Основные этапы развития письменности. Зарождение почты в Древнем мире. Почта в Западной Европе до конца XVIII в. Почта в России до середины XIX в. Промышленный переворот и его влияние на развитие почты. Почта в эпоху индустриализации
Раздел 3. Виды телеграфной связи и основные этапы ее развития.
Зарождение и развитие механического телеграфа. Предпосылки создания электрического телеграфа. Совершенствование электромагнитного телеграфа (Зёммеринг, Шиллинг, Уитстон, Кук, Морзе, Д.Юз). Распространение телеграфа как средства связи. Совершенствование телеграфа – появление многократного и частотного, многоканального телеграфирования
Раздел 4. Возникновение, распространение и совершенствование телефонной связи.
Изобретение телефона (Ч. Пейдж, И.Ф. Рейс, Э. Грей, А. Белл). Совершенствование микрофона. Создание и развитие телефонной коммутации. Распространение телефонной связи. Борьба с помехами - подготовка цифровой революции. Оптико-волоконная связь.
Раздел 5. Изобретение радио, освоение радиоэфира и основные виды радиосвязи.
Изобретение радио: А.С. Попов или Г. Маркони? Освоение радиоэфира. Изобретение и совершенствование электронной лампы. Возникновение и развитие радиовещания. Возникновение и развитие радиолокации. Спутниковая связь. Изобретение и развитие мобильной связи.
Раздел 6. Создание и совершенствование телевидения.
Первые опыты передачи изображения на расстояние. Изобретение Александра Бейна. Создание фототелеграфа. У истоков телевидения: от Артура Корна к Борису Розингу. Создание электромеханического телевидения. Изобретение электронного телевидения.

Переход от черно-белого к цветному телевидению. Телевидение на современном этапе.
Раздел 7. Изобретение компьютера и создание интернета.
Простейшие механические счетные устройства. Счетные машины Б. Паскаля и Г.В. Лейбница. Первые электро-механические счетные машины. Электромеханические счетные машины Г. Эйкена и К. Цузе. Изобретение первой ЭВМ. Пять поколений компьютера. Советские ЭВМ. Изобретение и совершенствование Интернета. Итоги третьей информационной революции.

Общая трудоемкость дисциплины

72 час(ов), 2 ЗЕТ

Форма промежуточной аттестации

Зачет

Б1.Б.10 Основы научных и экспериментальных исследований

Цели освоения дисциплины

Целью преподавания дисциплины «Основы научных и экспериментальных исследований» является:
формирование у обучающихся способности творчески мыслить, самостоятельно выполнять научно-исследовательские работы, анализировать и обобщать экономическую информацию

Место дисциплины в структуре ОП

Дисциплина «Основы научных и экспериментальных исследований» Б1.Б.10 является одной из дисциплин базовой части учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». 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:

– способностью к самоорганизации и самообразованию (ОК-8)

Содержание дисциплины

Раздел 1. Наука и ее роль в развитии общества
Основные подходы к определению понятий «наука», «научное знание». Отличительные признаки науки. Наука как система. Процесс развития науки. Цель и задачи науки. Субъект и объект науки. Классификация наук. Характерные особенности современной науки.
Раздел 2. Научное исследование и его этапы
Определение научного исследования. Цели и задачи научных исследований, их классификация по различным основаниям. Основные требования, предъявляемые к научному исследованию. Формы и методы научного исследования. Теоретический уровень исследования и его основные элементы. Эмпирический уровень исследования и его особенности. Этапы научно-исследовательской работы. Правильная организация научно-исследовательской работы.
Раздел 3. Методологические основы научного знания
Понятие методологии научного знания. Уровни методологии. Метод, способ и методика. Общенаучная и философская методология: сущность, общие принципы. Классификация общенаучных методов познания. Общелогические, теоретические и эмпирические методы исследования.
Раздел 4. Планирование научно-исследовательской работы
Формулирование темы научного исследования. Критерии, предъявляемые к теме научного исследования. Постановка проблемы исследования, ее этапы. Определение цели и задач исследования. Планирование научного исследования. Рабочая программа и ее структура. Субъект и объект научного исследования. Интерпретация основных понятий. План и его виды. Анализ теоретико-экспериментальных исследований. Формулирование выводов.
Раздел 5. Научная информация: поиск, накопление, обработка
Определение понятий «информация» и «научная информация». Свойства информации. Основные требования, предъявляемые к научной информации. Источники научной информации и их классификация по различным основаниям. Информационные потоки. Работа с источниками информации. Универсальная десятичная классификация. Особенности работы с книгой.
Раздел 6. Техническое и интеллектуальное творчество и его правовая охрана
Патент и порядок его получения. Изобретение, полезные модели, промышленные образцы: определения, условия патентоспособности, правовая охрана. Особенности патентных исследований. Последовательность работы при проведении патентных исследований. Интеллектуальная собственность и ее защита.
Раздел 7. Внедрение научных исследований и их эффективность
Процесс внедрения НИР и его этапы. Эффективность научных исследований. Основные виды эффективности научных исследований. Экономический эффект от внедрения научно-исследовательских разработок. Оценка эффективности исследований.
Раздел 8. Общие требования к научно-исследовательской работе
Структура научно-исследовательской работы. Способы написания текста. Язык и стиль экономической речи. Оформление таблиц, графиков, формул, ссылок. Подготовка рефератов и докладов. Подготовка и защита курсовых, дипломных работ. Рецензирование.

Общая трудоемкость дисциплины

72 час(ов), 2 ЗЕТ

Форма промежуточной аттестации

Зачет

Б1.Б.11 Введение в профессию

Цели освоения дисциплины

Целью преподавания дисциплины «Введение в профессию» является:
изучение сферы своей будущей деятельности, подготовка к выбору профиля своего дальнейшего обучения.

Место дисциплины в структуре ОП

Дисциплина «Введение в профессию» Б1.Б.11 является одной из дисциплин базовой части учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Алгоритмизация и программирование».

Требования к результатам освоения

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

– способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики (ОК-5)
– способностью анализировать физические явления и процессы для решения профессиональных задач (ОПК-1)
– способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности (ПК-9)

Содержание дисциплины

Раздел 1. История высшего образования в России и мире. Профессор М.А.Бонч-Бруевич. СПбГУТ. Факультет ИКСС. Кафедра ЗСС
История образо0вания 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 бакалавров 11.03.02 Инфокоммуникационные технологии и системы связи , профиль Защищенные системы и сети связи
Рассматривается роль и место подготовки бакалавра по профилю «Защищенные системы и сети связи». Рассматривается структура учебного плана, содержание дисциплин. Приводится анализ потребности в специалистах данного профиля на рынке труда.
Раздел 3. Криптография в истории. От древнего мира до настоящего времени
История криптографии. Первые шифры. Библейский шифр, шифры Цезаря, Виженера, трафаретная 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 компьютерные сети
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

72 час(ов), 2 ЗЕТ

Форма промежуточной аттестации

Зачет

Б1.Б.12.01 Математика

Цели освоения дисциплины

Целью преподавания дисциплины «Математика» является:
формирование знаний, умений и навыков, позволяющих проводить самостоятельный анализ проблем, возникающих в различных областях профессиональной деятельности.

Место дисциплины в структуре ОП

Дисциплина «Математика» Б1.Б.12.01 является базовой дисциплиной цикла учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Изучение дисциплины «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:

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

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

396 час(ов), 11 ЗЕТ

Форма промежуточной аттестации

Экзамен

Б1.Б.12.02 Дискретная математика

Цели освоения дисциплины

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

Место дисциплины в структуре ОП

Дисциплина «Дискретная математика» Б1.Б.12.02 является базовой дисциплиной цикла учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». 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:

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

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. Предикаты и кванторы. Полнота и замкнутость.
Понятия о предикатах и кванторах. Полнота и замкнутость. Полные системы булевых

функций
Раздел 4. Комбинаторика
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.
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.Б.12.03 Теория вероятностей и математическая статистика

Цели освоения дисциплины

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

Место дисциплины в структуре ОП

Дисциплина «Теория вероятностей и математическая статистика» Б1.Б.12.03 является базовой дисциплиной цикла учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Изучение дисциплины «Теория вероятностей и математическая статистика» основывается на базе знаний, умений и компетенций, полученных студентами в ходе освоения школьных курсов.

Дисциплина «Теория вероятностей и математическая статистика» Б1.Б.12.03 является одной из дисциплин базовой части учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Линейная алгебра и геометрия»; «Математика».

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

180 час(ов), 5 ЗЕТ

Форма промежуточной аттестации

Экзамен

Б1.Б.12.04 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 инфотелекоммуникаци, фотоники и оптоинформатики .

Место дисциплины в структуре ОП

Дисциплина «Теория информации» Б1.Б.12.04 является одной из дисциплин базовой части учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Дискретная математика»; «Информатика»; «Линейная алгебра и геометрия»; «Математика»; «Теория вероятностей и математическая статистика».

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. 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. : Передача видеосигналов: форматирование 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 базисных сигналов, нормы, скалярного произведения сигналов, ортогональности сигналов, ортонормированного базиса сигналов. Алгебраическая структура пространства сигналов. Геометрическая структура пространства сигналов. Энергия сигнала. Метрика пространства сигналов. Скалярное произведение сигналов. Обобщенный ряд Фурье.
Раздел 3. Спектры периодических и непериодических сигналов. Преобразование Фурье
Спектры периодических сигналов. Формы спектрального представления периодического сигнала: квадратурная, амплитудно-фазовая, комплексная.Понятие отрицательной частоты в спектре вещественного сигнала. Модель непериодического сигнала как предельного случая периодического сигнала , когда период повторения стремится к бесконечности. Прямое и обратное преобразование Фурье. Физический смысл спектральной плотности сигнала. Математический и физический спектр непериодического сигнала. Свойства преобразования Фурье.
Раздел 4. Спектрально-корреляционный анализ детерминированных сигналов в инфотелекоммуникации.
Энергетические модели сигналов.Корреляционные модели детерминированных сигналов. Свертка сигналов.Аналитический сигнал.Распределение энергии в спектре непериодического сигнала. Равенство Парсеваля и обобщенная формула Рэлея. Энергетический спектр сигнала. Распределение энергии в спектре вещественного непериодического сигнала. Эффективная ширина спектра сигнала. Корреляционные модели детерминированныхсигналов. Автокорреляционная функция вещественного сигнала (АКФ)и ее свойства. Связь АКФ сигнала с его энергетическим спектром. АКФ периодического вещественного сигнала. Свертка сигналов. 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.

Преобразование Гильберта. Спектральная плотность аналитического сигнала. Преобразование Гильберта во временной области. Преобразование Гильберта во частотной области. Преобразование Гильберта для гармонических сигналов.Понятие узкополосного 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 начальной фазы.

Раздел 6. Дискретные сигналы в радиотехнике и телекоммуникации

Дискретизация аналогового сигнала.Теорема Котельникова. Дискретное преобразование Фурье.Дискретизация 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 спектров при дискретизации. 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.

Раздел 8. Модуляция сигналов в радиотехнике и телекоммуникации.

Принципы модуляции сигналов. Аналоговая модуляция сигналов. Амплитудная модуляция сигналов. Балансная модуляция сигналов. Общие сведения о модуляции. Несущий сигнал и информационный сигнал. Шкала частот гармонического несущего сигнала Виды аналоговой модуляции: угловая модуляция(ЧМ, ФМ,), мгновенная полная фаза, мгновенная частота. Временные и векторные диаграммы модулированых сигналов. Спектры модулированных сигналов, спектр однотонального АМ сигнала. Демодуляция АМ сигнала. Амплитудное детектирование, квадратичное детектирование (нелинейное преобразование в режиме малого сигнала). Балансная модуляция сигналов и подавление несущего сигнала. Универсальный квадратурный модулятор. Формирование комплексной огибающей (Baseband signal).

Раздел 9. Принципы цифровой модуляции сигналов в телекоммуникациях

Цифровая модуляция сигналов. Сигналы с дискретной амплитудной модуляцией. Дискретная частотная модуляция сигналов. Дискретная фазовая и относительная фазовая модуляция сигналов. Дискретная квадратурная модуляция сигналов.Технологии и виды цифровой модуляции в современных системах связи. Цифровая бинарная модуляция: один символ - один бит. Сигнальные созвездия, фазовая плоскость синфазной I и квадратурной Q компонент. Цифровая квадратурная модуляция КАМ 16: один символ – 4 бита в той же полосе частот.Код Грея. Решетчатая модуляция. Сигнальные-кодовые конструкции цифровых сигналов. Помехоустойчивость различных видов модуляции.

Раздел 10. Спектральная и энергетическая эффективность систем телекоммуникаций.

Скорость передачи бит и частотный ресурс. Спектральная эффективность. МСИ в системах связи с цифровой модуляцией, глазковая диаграмма. Частотное ортогональное мультиплексирование и его реализация в системах связи. Отношение сигнал помеха по

мощности и особенности помех в каналах связи. Энергия бита и спектральная плотность аддитивной гауссовой помехи в виде белого шума. Энергетическая эффективность систем телекоммуникаций, помехоустойчивость инфотелекоммуникационных систем с аналоговыми и цифровыми видами модуляции.

Раздел 11. Анализ линейных систем во временной и частотной области

Временные и частотные характеристики линейных систем. 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. Прохождение белого шума через узкополосную систему.

Раздел 12. Математические модели случайных процессов. Прохождение случайных процессов через линейные цепи

Математические модели случайных сигналов. фунция распределения вероятности и плотность распределения вероятности стохастического сигнала. Моментные числовые характеристики закона распределения вероятности: математическое ожидание. дисперсия, автокорреляционная функция.Стационарные и эргодические случайные процессы. 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 13. Информационные характеристики источников сообщений и каналов. Энтропия и количество информации

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: энтропия - 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, избыточность сообщения, производительность источника. Информационные характеристики каналов: скорость передачи информации, максимальная скорость передачи информации (пропускная способность канала), коэффициент использования канала. Модели источников дискретных сообщений. Свойства эргодических источников. И 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 сообщений. Дифференциальная энтропия. Энтропия равномерного распределения. Энтропия гауссовского белого шума. Эпсилон - энтропия и эпсилон — производительность источника. Информационные характеристики непрерывных каналов. Модели непрерывных каналов. Скорость передачи информации и пропускная способность. Сравнение пропускных способностей дискретных и непрерывных каналов.

Раздел 14. Основы теории передачи информации с кодированием сообщений.

Способы кодирования. Префиксные коды, неравенство Крафта. Предельные возможности эффективного кодирования дискретных сообщений.Основная теорема кодирования Шеннона для канала без помех.

Раздел 15. 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, равномерное кодирование, статистическое кодирование, кодирование по методу Шеннона-Фано, кодирование по методу Хафмена, теорема Шеннона о кодировании источника независимых сообщений, условие оптимальности кодов. Словарное кодирование, алгоритм Лемпеля – Зива –Велча. Арифметическое кодирование.

Раздел 16. 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 17. Сверточные коды и декодер максимального правдоподобия.

Принципы работы сверточного кодера. Память кодера, кодовое ограничение, скорость кодирования. Сверточный кодер, как конечный автомат с памятью.Импульсная характеристика кодера, свободное расстояние ксверточного кода. Диаграмма состояний сверточного кодера, решетчатые диаграммы кодера. Декодирование сверточных кодов. Алгоритм декодирования по максимуму правдоподобия. Алгоритм декодирования Витерби.

Раздел 18. Основы оптимального приёма дискретных и непрерывных сообщений

Содержание и классификация задач оптимального приёма ДС. Оптимальный приём ДС в КС с детерминированной и стохастической структурой. Обнаружение и различение ДС. Критерии оптимального приёма ДС. Алгоритмы работы и структурные схемы оптимальных приёмников ДС в гауссовском КС. Синтез когерентного демодулятора ДС на фоне АБГШ. Согласованная фильтрация финитных во времени сигналов. Импульсная характеристика и передаточная частотная функция согласованного фильтра.

Раздел 19. Потенциальная помехоустойчивость приёма

Когерентное обнаружение и различение двоичных сигналов на фоне АБГШ. Потенциальная помехоустойчивость когерентного приема двоичных сигналов.Сравнение потенциальной помехоустойчивости сигналов с различными видами цифровой модуляции.Помехоустойчивость сигналов с квадратурной модуляцией. Особенности оценки помехоустойчивости некогерентных методов приема.

Раздел 20. Методы многоканальной передачи и распределения информации. Основные технологии в телекоммуникациях LTE и 5G.

Многопользовательская и многоканальная связь. Основы теории уплотнения и разделения сигналов в многоканальных системах. Многоканальная связь с временным, частотным, и кодовым уплотнением сигналов и доступом. Технология адаптивного изменения вида модуляции. Технология ортогонального частотного мультиплексирования.

Общая трудоемкость дисциплины

252 час(ов), 7 ЗЕТ

Форма промежуточной аттестации

Зачет, Экзамен. Курсовая работа

Б1.Б.12.05 Линейная алгебра и геометрия

Цели освоения дисциплины

Целью преподавания дисциплины «Линейная 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 «Линейная алгебра и геометрия» Б1.Б.12.05 является базовой дисциплиной цикла учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Изучение дисциплины «Линейная 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:

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

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

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

Б1.Б.13.01 Физика

Цели освоения дисциплины

Целью преподавания дисциплины «Физика» является:
фундаментальная подготовка студентов по физике, как средство общего когнитивного развития человека, способного к производственно-технологической и проектной деятельности, обеспечивающей модернизацию, внедрение и эксплуатацию различных средств связи и как база для изучения специальных дисциплин; 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 бакалавриата по направлению «10.03.01 Информационная безопасность».
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:

– способностью анализировать физические явления и процессы для решения профессиональных задач (ОПК-1)
– способностью применять соответствующий математический аппарат для решения профессиональных задач (ОПК-2)

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

396 час(ов), 11 ЗЕТ

Форма промежуточной аттестации

Экзамен

Б1.Б.13.02 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 части учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». 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:

– способностью применять положения электротехники, электроники и схемотехники для решения профессиональных задач (ОПК-3)

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.
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.Б.13.03 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.Б.13.03 является одной из дисциплин базовой части учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Физика»; «Электротехника».

Требования к результатам освоения

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

– способностью применять положения электротехники, электроники и схемотехники для решения профессиональных задач (ОПК-3)

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. Курсовой проект

Б1.Б.13.04 Физика (спецглавы)

Цели освоения дисциплины

Целью преподавания дисциплины «Физика (спецглавы)» является:
фундаментальная подготовка студентов по физике, как средство общего когнитивного развития человека, способного к производственно-технологической и проектной деятельности, обеспечивающей модернизацию, внедрение и эксплуатацию различных средств связи и как база для изучения специальных дисциплин; 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 оптики и квантовой физики, 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 (спецглавы)» Б1.Б.13.04 является одной из дисциплин базовой части учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Математика»; «Физика».

Требования к результатам освоения

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

– способностью анализировать физические явления и процессы для решения профессиональных задач (ОПК-1)
– способностью применять соответствующий математический аппарат для решения профессиональных задач (ОПК-2)

Содержание дисциплины

Раздел 1. Оптика
Законы геометрической оптики. Поляризация. Интерференция. Дифракция. Дисперсия.
Раздел 2. Квантовая физика
Тепловое излучение. Фотоны. Фотоэффект. Световое давление. Атом Бора. Гипотеза де Бройля. Соотношения неопределенностей. Уравнение Шредингера (общие свойства и конкретные ситуации).

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Экзамен

Б1.Б.14.01 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 овладения последующих дисциплин учебного плана

Место дисциплины в структуре ОП

Дисциплина «Информатика» Б1.Б.14.01 является базовой дисциплиной цикла учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность».
Изучение дисциплины «Информатика» основывается на базе знаний, умений и компетенций, полученных студентами в ходе освоения школьных курсов.

Требования к результатам освоения

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

– способностью анализировать физические явления и процессы для решения профессиональных задач (ОПК-1)

Содержание дисциплины

Раздел 1. Введение
Информатика, основные определение и термины, роль и значение вразвитиисовременного общества. Тенденции иперспективы развитияинформатики.Классификация и области применения.
Раздел 2. Информация
Понятие об информации. Виды и классификация информации.Требованияк информации. Методы и средства создания, приема, обработки,передачи,записи и хранения информации
Раздел 3. Вычислительная техника и программное обеспечение
Классификация технических средств. Этапы и тенденции современного развития. Электронные вычислительные машины (ЭВМ), конфигурация. Периферийное оборудование. Аппаратное, программное, информационное и математическое обеспечение компьютерных систем. Методы обработки информации в компьютерных системах.
Раздел 4. Основы программирования
Основы алгоритмизации. Основные определения и термины. Языки программирования. Классификация методов алгоритмизации. Сравнительные характеристики.
Раздел 5. Информационные системы
Информационная система, основные определения и термины. Классификация информационных систем. Структура исостав информационной системы. Проектирование информационнойсистемы. Базы данных. Компьютерные сети. Интернет. Угрозы и средства безопасности. Архивация данных

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

Б1.Б.14.02 Алгоритмизация и программирование

Цели освоения дисциплины

Целью преподавания дисциплины «Алгоритмизация и программирование» является:

изучение основ алгоритмизации вычислительных процессов, различных форм организации данных и алгоритмов работы с ними с использованием языка программирования высокого уровня.

Место дисциплины в структуре ОП

Дисциплина «Алгоритмизация и программирование» Б1.Б.14.02 является одной из дисциплин базовой части учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Введение в профессию»; «Информатика»; «Математика».

Требования к результатам освоения

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

– способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации (ОПК-4)

Содержание дисциплины

Раздел 1. Алгоритмы. Обозначения и способы записи.
Определение алгоритма. Способы описания алгоритмов. Элементы графического представления алгоритмов. Базовые алгоритмические конструкции: линейная, ветвление, цикл. Типовые алгоритмы обработки информации.
Раздел 2. Состав языка программирования. Типы данных.
Алфавит языка. Идентификаторы. Знаки операций. Выражения. Константы. Тип данных. Простые и составные типы данных. Операции с данными. Понятие массива. Переменные. Инициализация переменных. Интегрированная среда разработки.
Раздел 3. Базовые алгоритмические конструкции структурного программирования.
Порядок выполнения операторов в программе. Простой и составной оператор. Операторы

ветвления. Средства организации ветвлений на несколько направлений. Циклы с предусловием. Циклы с постусловием. Операторы передачи управления.
Раздел 4. Алгоритмизация ввода-вывода данных.
Организация ввода-вывода данных. Консольный ввод-вывод: средства ввода данных, средства вывода данных. Файловый ввод-вывод. Алгоритм вывода данных в файл. Алгоритм ввода данных из файла. Функции ввода-вывода.
Раздел 5. Функции как законченные алгоритмические конструкции.
Объявление и определение функций. Параметры функции. Возвращаемое значение функции. Глобальные и локальные переменные. Вызов функции. Структура программы.
Раздел 6. Указатели и массивы.
Массив как составной тип данных. Объявление массива, инициализация и обращение к элементам массива. Понятие указателя. Объявление указателя. Действия с указателями. Передача указателей функциям. Связь указателей с массивами.
Раздел 7. Алгоритмы работы с символьными строками.
Строка как символьный массив. Инициализация строк. Определение длины строки. Функции работы со строками. Типовые алгоритмы обработки строк: удаление символа, вставка символа (фрагмента строки), склеивание строк.
Раздел 8. Пользовательские типы данных.
Структуры: создание структуры, объявление структурной переменной, обращение к полям структуры, инициализация структурной переменной. Преобразование типов. Объединения. Перечисления.

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет. Курсовая работа

Б1.Б.14.03 Технологии и методы программирования

Цели освоения дисциплины

Целью преподавания дисциплины «Технологии и методы программирования» является:
ознакомление слушателей с основными возможностями языка программирования С++.

Место дисциплины в структуре ОП

Дисциплина «Технологии и методы программирования» Б1.Б.14.03 является одной из дисциплин базовой части учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». 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:

– способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации (ОПК-4)

Содержание дисциплины

Раздел 1. Основы C++
Основные понятия о структуре кода на языке C++: типы переменные, массивы, основные операторы, условные операторы, логические операторы, циклы, создание функций, указатели. Модели памяти.
Раздел 2. Работа со строками
Создание строк, обработка, сравнение, объединение стандартными средствами C++. Разбор специального класса String для работы со строками.
Раздел 3. Работа с тестовыми файлами
Создание текстового файла, открытие, редактирование, сохранение, поиск по файлу с помощью средств языка C++.
Раздел 4. Работа с бинарными файлами
Создание бинарного файла, открытие, редактирование, сохранение, поиск по файлу с помощью средств языка C++. Основные отличия от текстовых файлов.
Раздел 5. Рекурсивный вызов функции
Рекурсивный вызов функций. Разбор строки с математическим выражением и последующие его вычисление с помощью средств языка C++.
Раздел 6. Введение в понятие класса и объекта
Понятие структуры. Определение понятий класса, объекта класса, методы классов. Закрытая, открытая часть класса. Доступ к полям классов. Перегрузка функций, операторов.
Раздел 7. Наследование классов
Определение понятия наследования. Множественное наследование. Вложенные классы. Создание конструкторов и деструкторов классов.
Раздел 8. Безопасность кода
Уязвимость кода, защита от переполнения буфера, обработка кодов ошибок выполнения.

Общая трудоемкость дисциплины

180 час(ов), 5 ЗЕТ

Форма промежуточной аттестации

Экзамен

Б1.Б.14.04 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.Б.14.04 является базовой дисциплиной цикла учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Изучение дисциплины «Информационные технологии» 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 анализировать физические явления и процессы для решения профессиональных задач (ОПК-1)
– способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации (ОПК-4)

Содержание дисциплины

Раздел 1. Исторические и философские аспекты техники и технологий
Эволюция понятий “техника” и “технология”, являющихся основой современных исследований в области информационных технологий. Современные технологии. Информационная технология. Виды информационных технологий. Этапы развития информационных технологий. Классификация информационных технологий.
Раздел 2. Технологии обработки текстовой информации
Понятие «текст» как функционально-стилевая категория. Понятие документа, виды и форматы документов. Понятие трудоёмкости обработки текстовой информации для оценки эффективности использования основных технологий обработки текстовой информации. Характеристика техник и технологий решения базовых задач обработки текстовой информации средствами основных текстовых процессоров. Требования к оформлению рукописных работ (курсовых, дипломных работ и пр.).
Раздел 3. Технологии обработки экспериментальных данных средствами табличного процессора
Основные виды вычислительных задач. Методы решения задач обработки математической информации средствами табличного процессора. Характеристика техник

и технологий использования инструментальных средств, используемых для обработки математической информации. Применение функций, диаграмм и графиков.
Раздел 4. Технологии использования типовых моделей баз данных
Типовые модели баз данных и технологии их использования при решении практических задач обработки данных. Понятие системы, информационной системы, базы данных. Основные термины и понятия теории баз данных. Объекты реляционных баз данных: таблицы (отношения), запросы, формы, отчеты. Понятие целостности данных. Представление данных, языки запросов (QBE, SQL). Реляционные операторы.
Раздел 5. Технологии работы в глобальных компьютерных сетях. Облачные технологии
Адресация в сети Internet, принципы навигации в WWW, сервисы, предоставляемые Internet. Электронная почта и почтовые программы. Телеконференции. Браузеры. Поисковые системы. Особенности использования облачных технологий для реализации информационной системы предприятия или учреждения. Основные требования к информационной безопасности.
Раздел 6. Технологии подготовки презентаций
Требования, предъявляемые к подготовке материалов, и к оформлению презентаций. Структура слайда. Оформление слайда. Технология создания мультимедиа-презентаций: использование анимации, переход между слайдами по ссылке. Демонстрация презентации.
Раздел 8. Аттестация
Экзамен

Общая трудоемкость дисциплины

180 час(ов), 5 ЗЕТ

Форма промежуточной аттестации

Экзамен

Б1.Б.14.05 Аппаратные средства вычислительной техники

Цели освоения дисциплины

Целью преподавания дисциплины «Аппаратные средства вычислительной техники» является:
формирование у студентов профессиональной компетенции в областивычислительной и микропроцессорной техники, что позволит им проектироватьцифровые устройства любой степени сложности современными методами.

Место дисциплины в структуре ОП

Дисциплина «Аппаратные средства вычислительной техники» Б1.Б.14.05 является одной из дисциплин базовой части учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Исходный уровень

знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Дискретная математика»; «Информатика»; «Информационные технологии».

Требования к результатам освоения

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

– способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7)

Содержание дисциплины

Раздел 1. Введение
Предмет и задачи дисциплины. Цифровые устройства с аппаратной и программной логикой.
Раздел 2. Логические основы цифровой техники
Логические элементы. Методы записи алгоритмов. Синтез цифровых устройств.
Раздел 3. Типовые цифровые устройства комбинационного типа
Дешифраторы, шифраторы, кодопреобразователи, мультиплексоры, демультиплексоры, двоичные сумматоры, цифровые компараторы.
Раздел 4. Типовые цифровые устройства последовательностного типа
Триггеры, суммирующие, вычитающие, реверсивные счетчики, последовательные и параллельные регистры.
Раздел 5. Программируемая логика
Программируемые логические интегральные схемы (ПЛИС). Методы проектирования цифровых устройств на базе ПЛИС.
Раздел 6. Временные процессы в цифровых устройствах
Задержка распространения сигналов, быстродействие. Возникновение импульсных помех.
Раздел 7. Микропроцессорные системы (МПС)
Общая структура типовой микропроцессорной системы. Функционирование микропроцессорной системы.
Раздел 8. Память МПС
Память RAM и ROM, их разновидности, объединение микросхем памяти с целью увеличения разрядности и емкости, быстродействие памяти. Оперативная память, кэш-память, внешняя память.
Раздел 9. Взаимодействие МПС с внешней средой
Схемы программируемого интерфейса, их структура, подключение к шинам микропроцессораи внешним устройствам.
Раздел 10. Заключение
Перспективные направления проектирования вычислительных устройств.

Общая трудоемкость дисциплины

144 час(ов), 4 ЗЕТ

Форма промежуточной аттестации

Экзамен. Курсовой проект

Б1.Б.15.01 Информационное противоборство в современном мире

Цели освоения дисциплины

Целью преподавания дисциплины «Информационное противоборство в современном мире» является:
изучение вопросов роли информационной безопасности в современном мире.

Место дисциплины в структуре ОП

Дисциплина «Информационное противоборство в современном мире» Б1.Б.15.01 является базовой дисциплиной цикла учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Изучение дисциплины «Информационное противоборство в современном мире» основывается на базе знаний, умений и компетенций, полученных студентами в ходе освоения школьных курсов.

Дисциплина «Информационное противоборство в современном мире» Б1.Б.15.01 является одной из дисциплин базовой части учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». 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:

– способностью анализировать физические явления и процессы для решения профессиональных задач (ОПК-1)

Содержание дисциплины

Раздел 1. Истрия информационных войн в современном мире
История возникновения информационных войн как средства реализации государственных

интересов. Анализ крупнейших информационных войн современного мира. Оценка влияния информационных войн, их отражение в сознании российских граждан.
Раздел 2. Роль СМИ в информационных войнах
Средства массовой информации. Понятие, функции информационной войны, используемые методы. Роль средств массовой информации примере одной из информационных войн.
Раздел 3. Механизмы поиска информации. Поисковые роботы. Поисковые машины
Поисковый робот. Механизмы сбора новых данных о сайтах и их обновлениях. Поисковая система.
Раздел 4. Механизмы поиска информации в Интернет Google - основы поиска
Технологии поиска информации с помощью поисковой машины Google. Основные функции, возможности.
Раздел 5. Механизмы поиска информации. Индексация серверов, страничек, баз данных
World Wide Web (WWW). Механизмы поиска информации в интернет. Автономные поисковые работающие с индексами и работающие с каталогами. Индексация серверов, страничек, баз данных
Раздел 6. Скрытый интернет
Глубокая паутина (также известна как невидимая сеть) как множество веб-страниц Всемирной паутины, не индексируемых поисковыми системами.
Раздел 7. Скрытый интернет. Поиск
Поиск информации в скрытом интернете. Специальные поисковые машины и работа с ними.
Раздел 8. Конкурентная разведка. Анализ методат
Интернет-разведка (Competitive Intelligence). Перехват данных. Анализ методат. Выявление полезной информации.
Раздел 9. Автоматизированный поиск информации
Программирование поисковых машин на сбор мета-данных о web-страницах
Раздел 10. Социальные сети. Анонимизация деятельности в сети. Итоги изучения дисциплины
Методы и средства социальной инженерии. Сбор и анализ информации в социальных сетях. Методы сокрытия цифрового присутствия

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

Б1.Б.15.02 Организационное и правовое обеспечение информационной безопасности

Цели освоения дисциплины

Целью преподавания дисциплины «Организационное и правовое обеспечение информационной безопасности» является:
Целью преподавания дисциплины является изучение студентами на основе

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

Место дисциплины в структуре ОП

Дисциплина «Организационное и правовое обеспечение информационной безопасности» Б1.Б.15.02 является базовой дисциплиной цикла учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». 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:

– способностью использовать нормативные правовые акты в профессиональной деятельности (ОПК-5)
– способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-10)
– способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю (ПК-15)

Содержание дисциплины

Раздел 1. Правовое обеспечение информационной безопасности сетей и систем связи и пути его совершенствования. Задачи и функции правовой защиты информации
Национальные интересы РФ в информационной сфере и угрозы их безопасности. Цели, принципы, методы и средства правового обеспечения информационной безопасности РФ. Информационная среда как предмет правового регулирования. Закон РФ “Об информации, информатизации и защите информации” как основа регулирования правоотношений в области информатизации. Правовые основы организации деятельности государственных органов, обеспечивающих информационную безопасность РФ. Нормы законодательства РФ, регулирующие правовые отношения в сфере информационного обмена и обработки информации и позволяющие контролировать состояние безопасности сетей и систем связи, подключаемых к сети Интернет. Основные направления совершенствования правового обеспечения информационной безопасности сетей и систем связи. Особенности

раскрытия и расследования компьютерных преступлений. Информация как объект права. Понятие и виды защищаемой информации в сетях и системах связи. Основные термины в области правовой защиты информации. Понятие конфиденциальности, целостности и доступности информации. Правовые задачи, принципы и функции защиты информации информации в сетях и системах связи. Закон РФ “Об информации, информатизации и защите информации” об основах правового режима информационных ресурсов (фондов) и порядке их использования. Особенности разработки, производства и сертификации информационных систем, технологий и средств их обеспечения. Лицензирование деятельности по формированию и использованию информационных ресурсов (фондов).
Раздел 2. Основные законодательные акты, регулирующие отношения, связанные с правовой защитой и использованием интеллектуальной собственности. Защита информационных сетей и систем и прав на них
Общие положения Закона РФ “Об авторском праве и смежных правах”. Защита прав исполнителей, производителей фонограмм, организаций эфирного и кабельного вещания. Защита авторских и смежных прав. История развития законодательства о правовой охране программ для ЭВМ и баз данных. Порядок регистрации программ для ЭВМ и баз данных. Порядок передачи прав на использование программ для ЭВМ и баз данных по авторскому (лицензионному) договору. Понятие и виды информационных систем. Информационная война как целенаправленное информационное воздействие на информационные системы. Типовая стратегия информационной войны. Последствия информационной войны. Особенности правовой защиты информации в сетях и системах связи .
Раздел 3. Организационные источники и каналы утечки информации в сетях и системах. Силы, средства и условия организационной защиты информации
Национальные интересы РФ в информационной сфере и угрозы их безопасности. Цели, принципы, методы и средства правового обеспечения информационной безопасности РФ. Информационная среда как предмет правового регулирования. Закон РФ “Об информации, информатизации и защите информации” как основа регулирования правоотношений в области информатизации. Правовые основы организации деятельности государственных органов, обеспечивающих информационную безопасность РФ. Нормы законодательства РФ, регулирующие правовые отношения в сфере информационного обмена и обработки информации и позволяющие контролировать состояние безопасности сетей и систем связи, подключаемых к сети Интернет. Основные направления совершенствования правового обеспечения информационной безопасности сетей и систем связи. Особенности раскрытия и расследования компьютерных преступлений. Информация как объект права. Понятие и виды защищаемой информации в сетях и системах связи. Основные термины в области правовой защиты информации. Понятие конфиденциальности, целостности и доступности информации. Правовые задачи, принципы и функции защиты информации информации в сетях и системах связи. Закон РФ “Об информации, информатизации и защите информации” об основах правового режима информационных ресурсов (фондов) и порядке их использования. Особенности разработки, производства и сертификации информационных систем, технологий и средств их обеспечения. Лицензирование деятельности по формированию и использованию информационных ресурсов (фондов).
Раздел 4. Особенности системы организационной защиты информации, составляющей государственную и коммерческую тайну
Требования к безопасности информации в сетях и системах связи. Защита инфокоммуникаций от несанкционированного доступа к информации. Структура и принципы функционирования современных сетей и систем связи. Проблемы обеспечения безопасности обработки и хранения информации в сетях и системах связи. Базовые этапы

построения системы комплексной защиты сетей и систем связи. Управление системой защиты информации в сетях и системах связи. Функции ядра системы комплексной защиты. Многоуровневая структура системы защиты информации в сетях и системах связи на основе программно-аппаратных средств. Показатели защищенности от НСД к информации. Функции системы защиты по предупреждению угроз и устранению последствий их реализации. Классификация способов и средств комплексной защиты информации в сетях и системах связи. Компьютерные преступления. Политика безопасности. Модель мандатного доступа. Дискреционная политика. Матричная модель. Многоуровневые политики.
Раздел 5. Планирование процессов организационной защиты информации в сетях и системах Контроль функционирования системы организационной защиты информации
Сущность планирования как одной из основных функций управления системой организационной защиты информации информации в сетях и системах связи. Цели планирования. Оценка и анализ состояния системы ОЗИ как основа планирования. Стратегические и тактические планы. Соотношение планов ОЗИ с планами организации. Разновидности планов; их содержание и форма. Методы планирования. Особенности программно-целевого планирования. Сущность контроля как функции управления. Цели контроля. Функции контроля: сбор, обработка и анализ информации о фактических результатах деятельности по защите информации в сетях и системах связи, сравнение их с планами, выявление отклонений и анализ причин отклонений; разработка мероприятий, необходимых для достижения целей ОЗИ. Учет и отчетность по ОЗИ, как основа контроля. Объекты контроля. Методы контроля: анализ, наблюдение, проверка, сравнение, учет и др. Формы контроля: предварительный, текущий и заключительный. Технология контроля: выработка стандартов и критериев ОЗИ, сопоставление с ними полученных результатов и принятие необходимых корректирующих действий. Выбор методов контроля, используемых на различных его этапах в зависимости от объектов контроля.

Общая трудоемкость дисциплины

144 час(ов), 4 ЗЕТ

Форма промежуточной аттестации

Экзамен

Б1.Б.15.03 Техническая защита информации

Цели освоения дисциплины

Целью преподавания дисциплины «Техническая защита информации» 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 инженерно-

технических средствах защиты объектов, как изучаемых в настоящей дисциплине, так и находящихся за ее рамками.

Место дисциплины в структуре ОП

Дисциплина «Техническая защита информации» Б1.Б.15.03 является одной из дисциплин базовой части учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». 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:

– способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7)

Содержание дисциплины

Раздел 1. Введение
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 тревожно-вызывной 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

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

Б1.Б.15.04 Криптографические методы защиты информации

Цели освоения дисциплины

Целью преподавания дисциплины «Криптографические методы защиты информации» является:
Целью дисциплины является формирование у обучаемых знаний в области принципов криптографических преобразований, типовые программно-аппаратных средств криптографической защиты информации и инфокоммуникаций от несанкционированного доступа.

Место дисциплины в структуре ОП

Дисциплина «Криптографические методы защиты информации» Б1.Б.15.04 является базовой дисциплиной цикла учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Изучение дисциплины «Криптографические методы защиты информации» основывается на базе знаний, умений и компетенций, полученных студентами в ходе освоения школьных курсов.

Дисциплина «Криптографические методы защиты информации» Б1.Б.15.04 является одной из дисциплин базовой части учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». 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:

– способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7)

Содержание дисциплины

Раздел 1. Методы и средства криптографии в инфокоммуникациях
История криптографии. Основные понятия и определения. Требования к криптографическим системам. Исторические шифры. Современные методы и средства криптографии.
Раздел 2. Симметричные криптографические системы , использующие блоковые шифры.
Основные классы симметричных криптосистем. Общие сведения о блочных шифрах . Примеры алгоритмов блочного шифрования.:DES и его модификации, AES(Rijndael), . RC5.,Российский стандарт ГОСТ28147-89 . Режимы использования блочных шифров. Многократное шифрование
Раздел 3. Симметричные криптографические системы использующие потоковые шифры.
Особенности потоковых шифров. Свойства линейного рекуррентного регистра. Нелинейные узлы усложнения. Примеры алгоритмов потокового шифрования :RC4, A5/1.
Раздел 4. Симметричные криптографические системы использующие потоковые шифры.
Классификации систем аутентификации и характеристики их эффективности. Безусловно стойкие системы аутентификации. Вычислительно стойкие системы аутентификации. Использование модификаций блоковых шифров. Примеры систем аутентификаций , использующих блоковые шифры (ГОСТ28147 и др.)
Раздел 5. Основные принципы построения несимметричных криптосистем (криптосистем

с открытым ключом).
Основные требования , предъявляемые к криптосистемам с открытым ключом. Основы теории чисел и теории конечных полей. Свойства эллиптических кривых.
Раздел 6. Примеры построения криптосистем с открытым ключом
Криптосистемы : РША , Рабина, Эль-Гамаля, Диффи-Хеллмана , Мак-Элис. Построение криптосистем на основе теории эллиптических кривых. Использование сертификатов.
Раздел 7. Электронные (цифровые подписи) и криптографические протоколы..
Принцип построения цифровых подписей (ЦП) на основе использования криптосистем с открытым ключом. Определение и свойства криптографическихххещ-функций. Примеры построения ЦП :DSA, ГОСТ Р 3410-94.Понятие о криптографических протоколах. Примеры криптографических протоколов : разделение секретов , идентификация , совместные вычисления , тайное голосование. Методы формирования и распределения аутентифицированных ключей.

Общая трудоемкость дисциплины

180 час(ов), 5 ЗЕТ

Форма промежуточной аттестации

Экзамен

Б1.Б.15.05 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 «Программно-аппаратные 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.Б.15.05 является одной из дисциплин базовой части учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность».
Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких

дисциплин, как «Алгоритмизация и программирование»; «Введение в профессию».

Требования к результатам освоения

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

– способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7)
– способностью выбирать режимы работы программно-аппаратных средств защиты информации в компьютерных сетях (ПС-11)

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

144 час(ов), 4 ЗЕТ

Форма промежуточной аттестации

Экзамен

Б1.Б.15.06 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.Б.15.06 является одной из дисциплин базовой части учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». 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:

– способностью использовать нормативные правовые акты в профессиональной деятельности (ОПК-5)
– способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты (ПК-4)
– способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов (ПК-8)
– способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации (ПК-13)

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

180 час(ов), 5 ЗЕТ

Форма промежуточной аттестации

Экзамен

Б1.Б.15.07 Комплексное обеспечение защиты информации объекта информатизации

Цели освоения дисциплины

Целью преподавания дисциплины «Комплексное обеспечение защиты информации объекта информатизации» является:
формирование компетентности в области разработки комплексной системы защиты информации предприятия

Место дисциплины в структуре ОП

Дисциплина «Комплексное обеспечение защиты информации объекта информатизации» Б1.Б.15.07 является базовой дисциплиной цикла учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Изучение дисциплины «Комплексное обеспечение защиты информации объекта информатизации» основывается на базе знаний, умений и компетенций, полученных студентами в ходе освоения школьных курсов.

Дисциплина «Комплексное обеспечение защиты информации объекта информатизации» Б1.Б.15.07 является одной из дисциплин базовой части учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». 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:

– способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7)

– способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации (ПК-6)
– способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений (ПК-7)
– способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности (ПК-14)

Содержание дисциплины

Раздел 1. Введение в дисциплину. Сущность комплексной системы защиты информации и принципы ее организации
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.
Раздел 2. Методологические и концептуальные основы комплексной системы защиты информации.
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, технико-экономического обоснования. Технический проект, рабочий проект. Апробация системы защиты информации и ввод ее в эксплуатацию.

Раздел 9. Кадровое, материально-техническое 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 организационно-распорядительных 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.Б.16.01 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.Б.16.01 является базовой дисциплиной цикла учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Изучение дисциплины «Математические основы защиты информации» 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. 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.Б.16.02 Защищенные операционные системы

Цели освоения дисциплины

Целью преподавания дисциплины «Защищенные операционные системы» 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 «Защищенные операционные системы» Б1.Б.16.02 является базовой дисциплиной цикла учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Изучение дисциплины «Защищенные операционные системы» 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 определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7)
– способностью администрировать подсистемы информационной безопасности объекта защиты (ПК-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

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

Б1.Б.16.03 Вычислительные сети

Цели освоения дисциплины

Целью преподавания дисциплины «Вычислительные сети» является:
получить представление об архитектуре, структуре, функциях, компонентах и моделях сети Интернет и других компьютерных сетей

Место дисциплины в структуре ОП

Дисциплина «Вычислительные сети» Б1.Б.16.03 является базовой дисциплиной цикла учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Изучение дисциплины «Вычислительные сети» 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 определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7)

– способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1)

Содержание дисциплины

Раздел 1. Введение
Понятие компьютерной сети. Ресурсы в сети: клиент-серверные приложения, peer-to-peer приложения. LAN, WANи интернет. Подключение к сети Интернет. Современные подходы к организации сети. Конвергентные сети. BYOD, видео, аудио конвергенция. Основные угрозы сети.
Раздел 2. Работа с операционной системой Cisco IOS
Введение в CiscoIOS. Способы доступа к устройствам под управлением CiscoIOS.Навигация в CiscoIOS. Режимы работы (режим пользователя, привелигированный режим, режим глобальной конфигурации, подрежимы). Структура работы команд. Именование устройств. Ограничение доступа в режимы настройки (парольная защита). Схема сетевой адресации устройств. Конфигурирование IP-адресов конечных устройств.
Раздел 3. Сетевые протоколы и средства взаимодействия
Правила взаимодействия сетевых устройств. Сетевые протоколы. Взаимодействие между протоколами. Стек TCP/IP. Стандартизующие организации (IEEE, IETF, ISO). Модель взаимодействия сетевых устройств (OSI). Модель TCP/IP. Доставка сообщений. Доступ к локальным ресурсам (MAC-адреса и IP-адреса). Доступ к устройствам локальной подсети. Шлюз по умолчанию. Доступ к удаленным устройствам.
Раздел 4. Доступ к сети
Доступ к устройствам. Сетевые карты. Назначение физического уровня модели OSI. Среда передачи. Принципы первого уровня модели OSI (полоса пропускания, пропускная способность, типы кабелей). Медные кабели. Экранированная витая пара, коаксиальный кабель, оптоволокно. Неэкранированная витая пара. Дизайн оптических коннекторов, сравнение оптических и медных кабелей. Беспроводная среда передачи. Типы беспроводных локальных сетей. Стандарты Wi-fi (802.11a, b, g, n, ac). Канальный уровень. MAC-адреса. Физические и логические топологии. Режимы дуплекса. Структура кадра. Ethernet-кадр, PPP-кадр, 802.11 кадр.
Раздел 5. Протокол Ethernet
LLCиMACподуровни. Атрибуты Ethernet. Размер кадра Ethernet. MAC-адресация, одноадресная, многоадресная и широковещательная рассылка. Протокол ARP. Поиск неисправностей в протоколе ARP. Коммутаторы. Параметры дуплекса. Структура таблицы MAC-адресов. Методы обработки кадров. Типы коммутаторов (модульные, фиксированные). Многоуровневые коммутаторы. Настройка маршрутизируемых интерфейсов.
Раздел 6. Сетевой уровень
Протокол IP. Характеристики протокола IP. Структура протокола IPv4. Протокол IPv6. Структура заголовка IPv6. Структура протокола IPv6. Маршутизация пакетов. Таблицы маршрутизации протоколов IPv4, IPv6. Маршрутизатор Cisco. Компоненты маршрутизатора (материнская плата, процессор, память, интерфейсы). Загрузка маршрутизатора. Операционная система CiscoIOS.
Раздел 7. Транспортный уровень
Доставка данных. Роль транспортного уровня. Протоколы TCP, UDP. Сравнение протоколов транспортного уровня. Гарантированная доставка сегментов, механизмы

контроля трафика, коррекция ошибок. Адресация приложений. Нумерация портов. Анализ установки сессии протокола TCP (three-wayhandshake). Датаграммы UDP.
Раздел 8. IP-адресация
Введение. Двоичная и десятичная системы счисления. Перевод из двоичной системы счисления в десятичную и обратно. Маска подсети. Одноадресные, многоадресные, широковещательные типы адресов IPv4. Типы адресов IPv4 (публичные, приватные). Классы адресов. Назначение IP-адресов. IPv6-адресация. Потребность в IPv6, проблемы IPv4. Шестнадцатеричная система счисления. Правила адресации IPv6. Типы адресов IPv6. Понятие префикса. Назначение IP-адресов. Протоколы DHCPv4, v6. Расширение EUI-64. Сообщения ICMPv4, ICMPv6. Утилиты ping, traceroute.
Раздел 9. Подсети
Разработка плана IP-адресации. Расчет маски подсети. Маски переменной длины (VLSM). Подсети в протоколе IPv6.
Раздел 10. Уровень приложений
Уровни сессий и представлений модели OSI.Приложенияpeer-to-peer. Взаимодействие между уровнями приложений. Модель клиент-сервера. Протоколы HTTP, SMTP, POP3, IMAP. Протокол DNS. Протоколы DHCP, FTP. Интернет вещей. Конвергированные сети. Передача видео-трафика.
Раздел 11. Структура сети небольшого размера
Принципы организации сетей небольшого размера. Адресация устройств. Избыточность в сетях небольшого размера. Приложения сети. Приложения реального времени. Защита сетевых устройств. Физическая защита. Типы угроз. Виды сетевых атак (вирусы, черви, трояны). Средства защиты в сети. Фаерволы. Защита по паролю. Протоколы SSH, HTTPS, AAA.

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

Б1.Б.16.04 Криптографические протоколы

Цели освоения дисциплины

Целью преподавания дисциплины «Криптографические протоколы» является: изучение вопросов основ криптографической защиты информации в телекоммуникационных системах. Дисциплина «Криптографические протоколы» 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 «Криптографические протоколы» Б1.Б.16.04 является базовой дисциплиной цикла учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Изучение дисциплины «Криптографические протоколы» основывается на базе знаний, умений и компетенций, полученных студентами в ходе освоения школьных курсов.

Дисциплина «Криптографические протоколы» Б1.Б.16.04 является одной из дисциплин базовой части учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». 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:

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

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

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

Б1.Б.16.05 Ассемблер в задачах защиты информации

Цели освоения дисциплины

Целью преподавания дисциплины «Ассемблер в задачах защиты информации» является:
ознакомление слушателей с основными возможностями языка программирования Ассемблер.

Место дисциплины в структуре ОП

Дисциплина «Ассемблер в задачах защиты информации» Б1.Б.16.05 является базовой дисциплиной цикла учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность».
Изучение дисциплины «Ассемблер в задачах защиты информации» 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 определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7)

– способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2)

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

Экзамен

Б1.Б.16.06 Теоретические основы компьютерной безопасности

Цели освоения дисциплины

Целью преподавания дисциплины «Теоретические основы компьютерной безопасности» является:
Сформировать компетенции обучающегося в области защиты информации

Место дисциплины в структуре ОП

Дисциплина «Теоретические основы компьютерной безопасности» Б1.Б.16.06 является одной из дисциплин базовой части учебного плана подготовки

бакалавриата по направлению «10.03.01 Информационная безопасность». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Информационное противоборство в современном мире».

Требования к результатам освоения

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

– способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7)
– способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты (ПК-4)

Содержание дисциплины

Раздел 1. Технологии программной защиты в интернете
Сетевая безопасность, Инструментарий Хакера, Защита Windows-сервер
Раздел 2. Web-программирование в защите информации
Основы языка php, Различные инъекции и атаки
Раздел 3. Вредоносное программное обеспечение
Классификация вредоносного программного обеспечения, Антивирусные программы

Общая трудоемкость дисциплины

144 час(ов), 4 ЗЕТ

Форма промежуточной аттестации

Экзамен

Б1.Б.16.07 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.

Место дисциплины в структуре ОП

Дисциплина «Методы оценки безопасности компьютерных систем» Б1.Б.16.07 является базовой дисциплиной цикла учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Изучение дисциплины «Методы оценки безопасности компьютерных систем» 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 определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7)
– способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации (ПК-5)
– способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов (ПК-11)
– способностью принимать участие в проведении экспериментальных исследований системы защиты информации (ПК-12)

Содержание дисциплины

Раздел 1. Введение
Предмет и основные задачи дисциплины «Основы проектирования защищенных инфокоммуникационных систем», её значение в сис¬теме 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.Б.16.08 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.Б.16.08 является базовой дисциплиной цикла учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Изучение дисциплины «Защита программ и данных» 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 определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7)
– способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2)

Содержание дисциплины

Раздел 1. Методы экспериментов с черным ящиком
Динамический метод. Статический метод. Методы экспериментов с черным ящиком.
Раздел 2. Методы исследования программ
Искусственное усложнение алгоритмов обработки данных; Выявление фактов выполнения программы под отладчиком. Нестандартное обращение к функциям операционной системы;
Раздел 3. Особенности анализа программ
Особенности анализа графических программ; Особенности анализа параллельного кода; Особенности анализа кода в режиме ядра Windows
Раздел 4. Защита программ от анализа
Выявление факта выполнения программы под отладчиком. Искусственное усложнение алгоритмов обработки данных; Искусственное усложнение структуры программы;
Раздел 5. Модели взаимодействия программной закладки с атакуемой системой
Модификация машинного кода монитора безопасности. Порождение дочернего процесса системным процессом;
Раздел 6. Предпосылки к внедрению программ закладок
Уязвимость переполнения буфера; Уязвимость "отсутствие необходимых проверок входных данных";
Раздел 7. Методы внедрения программных закладок
Маскировка программной закладки под системное программное обеспечение; Подмена системного программного обеспечения;
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

2. Аннотации рабочих программ дисциплин (модулей) вариативной части

Б1.В.01.01 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.01.01 является обязательной дисциплиной вариативной части блока 1 учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Изучение дисциплины «Безопасность Astra Linux» опирается на знании дисциплин(ы) .

Требования к результатам освоения

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

– способностью администрировать подсистемы информационной безопасности объекта защиты (ПК-3)
– способностью формулировать и настраивать политики безопасности операционных систем (ПС-1)

– способностью противодействовать угрозам безопасности информации с использованием встроенных средств защиты информации операционных систем (ПС-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.01.02 Защита информации в центрах обработки данных

Цели освоения дисциплины

Целью преподавания дисциплины «Защита информации в центрах обработки данных» 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. 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 информации в центрах обработки данных» Б1.В.01.02 является обязательной дисциплиной вариативной части блока 1 учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Изучение дисциплины «Защита информации в центрах обработки данных» опирается на знании дисциплин(ы) «Цифровая криминалистика».

Требования к результатам освоения

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

– способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений (ПК-7)
– способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности (ПК-9)
– способностью формулировать и настраивать политики безопасности операционных систем (ПС-1)

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
Уязвимость кода, защита от переполнения буфера, обработка кодов ошибок выполнения.
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
Уязвимость кода, защита от переполнения буфера, обработка кодов ошибок выполнения.

Общая трудоемкость дисциплины

144 час(ов), 4 ЗЕТ

Форма промежуточной аттестации

Экзамен

Б1.В.02.01 Основы маршрутизации в компьютерных сетях

Цели освоения дисциплины

Целью преподавания дисциплины «Основы маршрутизации в компьютерных сетях» является:
дисциплины является получение фундаментальныхзнаний в области организации локальных вычислительных сетей. Рассматриваютсямодели 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.02.01 является обязательной дисциплиной вариативной части блока 1 учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Изучение дисциплины «Основы маршрутизации в компьютерных сетях» опирается на знании дисциплин(ы) «Вычислительные сети».

Требования к результатам освоения

Процесс изучения дисциплины направлен на формирование следующих компетенций:

В соответствии с ФГОС:

– способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1)
– способностью проводить мониторинг функционирования программно-аппаратных средств защиты информации в компьютерных сетях (ПС-12)

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

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Экзамен

Б1.В.02.02 Принципы организации локальных вычислительных сетей

Цели освоения дисциплины

Целью преподавания дисциплины «Принципы организации локальных вычислительных сетей» является:
получение фундаментальных знаний в области организации локальных вычислительных сетей. Рассматриваются модели взаимодействия сетевых устройств. Получение знаний в области функционирования операционной системы Cisco IOS

Место дисциплины в структуре ОП

Дисциплина «Принципы организации локальных вычислительных сетей» Б1.В.02.02 является обязательной дисциплиной вариативной части блока 1 учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Изучение дисциплины «Принципы организации локальных вычислительных сетей» опирается на знании дисциплин(ы) «Вычислительные сети».

Требования к результатам освоения

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

– способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1)
– способностью обосновывать выбор используемых программно-аппаратных средств защиты информации в компьютерных сетях (ПС-9)

Содержание дисциплины

Раздел 1. Суммаризация соединений
Основные концепции суммаризации соединений. Технология EtherChannel. Протоколы PAGP, LACP. Настройка EtherChannel. Поиск неисправностей сетей с протоколом EtherChannel.
Раздел 2. Введение в масштабируемые сети
Иерархический дизайн сетей. Архитектура Cisco Enterprise. Расширение сети. Планирование избыточной топологии. Расширение уровня доступа. Платформы коммутаторов. Плотность портов. PoE. Многоуровневая коммутация. Платформы маршрутизаторов. Работа с CiscoIOS. Управление с образами CiscoIOS. Лицензирование.
Раздел 3. Избыточность локальных сетей
Назначение протокола связующего дерева STP. Проблемы коммутируемых сетей: MAC-штормы, широковещательные штормы, дублицированные копии одноадресных рассылок. Работа алгоритма STP. Понятие BPDU. Протокол PVST+. Протокол RPVST+. Конфигурация протокола RapidSpanningTree. Протоколы FHRP (HSRP, VRRP, GLBP).
Раздел 4. Беспроводные локальные сети
Основные концепции беспроводных локальных сетей. Поддержка функций мобильности. Беспроводные технологии. Стандарты 802.11. Сертификация Wi-fi. Сравнение WLANи LAN. Беспроводные адаптеры. Антенны. Внедрение беспроводной сети. Топологии 802.11 (Ad-hoc, infstructuremode). Принцип работы беспроводной точки доступа. Аутентификация. Планирование внедрения WLAN. Типы основных угроз (man-in-the-middle, DoS атаки и др.) Защита беспроводных сетей (методы проверки подлинности, методы шифрации). Настройка беспроводного маршрутизатора. Настройка беспроводных клиентов. Поиск неисправностей в беспроводных сетях WLAN.
Раздел 5. Тонкая настройка и поиск неисправностей в протоколе OSPF
Преимущества настройки протокола OSPFдля одной области. Проверка работы OSPFv3. Работа OSPFв многоадресных сетях. Выбор DR/BDR. Пропаганда шлюза по умолчанию в протоколе OSPF. Настройка интервалов Hello и dead таймеров. Защита протокола OSPF. Настройка аутентификации MD5.Балансировка нагрузки. Поиск неисправностей в сети, работающей под управлением протокола OSPF
Раздел 6. Настройка протокола OPSF для нескольких областей
Типы маршрутов протокола OSPF (LSA 1,2,3,4,5,7). Таблицы маршрутизации протокола OSPF. Внедрение протокола OSPFдля нескольких областей. Внутренние и внешние маршруты. Суммаризация маршрутов. Проверка сети OSPF для нескольких областей.
Раздел 7. Настройка протокола EIGRP
Основные функции протокола EIGRP. Типы пакетов EIGRP. Настройка протокола EIGRPдля ipv4. Понятие автономной системы. Объявление сетей. Проверка функционирования протокола EIGRP. Работа EIGRP. Конвергенция. Метрика протокола. Алгоритм DUAL. Понятие Successor, feasible successor. Таблицы соседей, топологии. Настройка EIGRP для IPv6. Проверка работоспособности протокола EIGRP.
Раздел 8. Дополнительная настройка протокола EIGRP
Сетевая топология. Настройка суммаризации маршрутов. Пропаганда шлюза по умолчанию. Балансировка протокола EIGRP.Настройка аутентификации MD5. Поиск и устранение неисправностей в настройке протокола EIGRP.
Раздел 9. Образы Cisco IOS и лицензирование
Администрирование образов Cisco IOS. Различие в семействе операционных систем (релиз 12 и 15 IOS). Правила именования образов. Администрирование образов Cisco IOS. Копирование образа Cisco IOS. Процесс загрузки. Лицензирование Cisco IOS. Проверка установленной лицензии.

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет. Курсовая работа

Б1.В.02.03 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.02.03 является обязательной дисциплиной вариативной части блока 1 учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». 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:

– способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1)
– способностью проводить мониторинг функционирования программно-аппаратных средств защиты информации в компьютерных сетях (ПС-12)

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.03.01 Разработка защищенного программного обеспечения

Цели освоения дисциплины

Целью преподавания дисциплины «Разработка защищенного программного

обеспечения» является:
изучение принципов построения безопасного кода на языке программирования Java, использования и разработки собственных функций обеспечения информационной безопасностью.

Место дисциплины в структуре ОП

Дисциплина «Разработка защищенного программного обеспечения» Б1.В.03.01 является обязательной дисциплиной вариативной части блока 1 учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Изучение дисциплины «Разработка защищенного программного обеспечения» опирается на знании дисциплин(ы) «Введение в профессию».

Требования к результатам освоения

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

– способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2)
– способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов (ПК-11)
– способностью формулировать и обосновывать правила безопасной эксплуатации программного обеспечения (ПС-14)

Содержание дисциплины

Раздел 1. Введение в Java
Язык Java как средство программирования, преимущества, характерные особенности. Язык Java и Интернет. Отличия от C++. Типы данных, арифметические, логические, условные операторы и операторы цикла. Одномерные и многомерные массивы. Примеры простых программ.
Раздел 2. Основы объектно-ориентированного программирования
Введение в концепцию объектно-ориентированного программирования, основные понятия, особенности реализации. Объявления классов. Основные компоненты класса: поля, методы, конструкторы. Вводится понятие наследования, полиморфизма. Обобщённые типы данных.Общие сведения об исключениях, обработка исключений с помощью конструкции try/catch/finally.Создание собственного исключения. Алгоритм обработки ошибок.
Раздел 3. Потоки ввода-вывода
Ввод-вывод данных в консольном и графическом режиме.форматирование вывода, считывание ввода. Работа с потоками. Работа с текстовыми и бинарными файлами. Работа с сетью TCP/IP. Многопоточное программирование
Раздел 4. Графический интерфейс

Создание окон, кнопок на окне, полей вывода, ввода, поля для рисования. Включение скроллинга. Менеджеры компоновки.
Раздел 5. Обработка событий
Знакомство с методами обработки событий в Java: нажатие кнопки, движение мыши, нажатию кнопки на клавиатуре и д.р. с помощью интерфейсов.
Раздел 6. Структура байт кода
Компиляция .javав .class., структура файла .class: заголовок; пул констант; объявления класса; поля методы; имена типов, методов и классов; исполняемый код. Примеры соответствия кода и байт кода
Раздел 7. Основные механизмы обеспечения безопасности
Введение в основные механизмы встроенные в виртуальную машину JRE: загрузчики классов, верификация байт кода, диспетчеры полномочий, аутентификация пользователей, цифровые подписи, цифровые сертификаты, алгоритмы шифрования.
Раздел 8. Цифровые водяные знаки в исполнимых файлах
Введение в основы вложения сообщений в исполняемый код. Рассмотрены особенности вложение в отличие от классических покрывающих сообщений. Применение вложений в качестве цифровых водяных знаков.

Общая трудоемкость дисциплины

144 час(ов), 4 ЗЕТ

Форма промежуточной аттестации

Экзамен

Б1.В.03.02 Реверс-инжиниринг системного программного обеспечения

Цели освоения дисциплины

Целью преподавания дисциплины «Реверс-инжиниринг системного программного обеспечения» является:
изучение обратный инжиниринг, реверс-инжиниринг. Кроме того, студенты исследуют свойства готовых устройств или программ, а также документацию на него с целью понять принцип его работы;

Место дисциплины в структуре ОП

Дисциплина «Реверс-инжиниринг системного программного обеспечения» Б1.В.03.02 является обязательной дисциплиной вариативной части блока 1 учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Изучение дисциплины «Реверс-инжиниринг системного программного обеспечения» опирается на знании дисциплин(ы) «Дискретная математика».

Требования к результатам освоения

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

– способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2)
– способностью анализировать функционирование программного обеспечения с целью определения возможного вредоносного воздействия (ПС-15)
– способностью определять порядок функционирования программного обеспечения с целью обеспечения защиты информации (ПС-17)

Содержание дисциплины

Раздел 1. Взлом программного обеспечения
Виды взлома, принципы взлома, правовые аспекты деятельности
Раздел 2. Виды реинжиниринга
Рефакторинг, Машинно-независимая оптимизация, Распараллеливание, Машинно-зависимая оптимизация, Обфускация
Раздел 3. Методы и инструменты реинжиниринга
Системы перезаписи (rewriting systems), Универсальные системы преобразования программ
Раздел 4. Обратная разработка
Исследование свойств программы, воспроизведение программы или иного объекта с аналогичными функциями, но без копирования как такового.
Раздел 5. Обратная инженерия
процессы систематического разбора программы (восстановления её исходного текста и структуры), изучения алгоритмов, добавления новых возможностей, восстановления протоколов или исправления ошибок.
Раздел 6. Дизассемблирование
Дизассемблирование машинного кода программы для получения её листинга на языке ассемблера.
Раздел 7. Декомпиляторы
Декомпиляция машинного или байт-кода программы для создания исходного кода на некотором языке программирования высокого уровня.

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

Б1.В.03.03 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.03.03 является обязательной дисциплиной вариативной части блока 1 учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». 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:

– способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2)
– способностью устанавливать и настраивать антивирусные средства защиты информации в операционных системах (ПС-5)

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

180 час(ов), 5 ЗЕТ

Форма промежуточной аттестации

Экзамен. Курсовая работа

Б1.В.ДВ.01.01 Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации

Цели освоения дисциплины

Целью преподавания дисциплины «Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации» является:
Цель изучения учебной дисциплины «Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации»

Место дисциплины в структуре ОП

Дисциплина «Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации» Б1.В.ДВ.03.02 является дисциплиной по выбору вариативной части блока 1 учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». 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:

– способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов (ПК-8)
– способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-10)
– способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности (ПК-14)

– способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю (ПК-15)

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 здоровью и развитию".

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Экзамен

Б1.В.ДВ.01.02 Нормативные документы

Цели освоения дисциплины

Целью преподавания дисциплины «Нормативные документы» является:
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, основных положениях институтов информационного права, отраженных в нормативно-правовых актах, выработку навыков и умений, необходимых для профессионального выполнения поставленных задач.

Место дисциплины в структуре ОП

Дисциплина «Нормативные документы» Б1.В.ДВ.03.04 является дисциплиной по выбору вариативной части блока 1 учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Защищенный электронный документооборот».

Требования к результатам освоения

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

– способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов (ПК-8)
– способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-10)
– способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности (ПК-14)
– способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю (ПК-15)

Содержание дисциплины

Раздел 1. 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 2. 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 3. 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 4. 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 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 здоровью и развитию".

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Экзамен

Б1.В.ДВ.02.01 Основы проектирования защищенных инфокоммуникационных систем

Цели освоения дисциплины

Целью преподавания дисциплины «Основы проектирования защищенных инфокоммуникационных систем» является:
изучение вопросов основ защиты информации в телекоммуникационных системах.

Место дисциплины в структуре ОП

Дисциплина «Основы проектирования защищенных инфокоммуникационных систем» Б1.В.ДВ.02.04 является дисциплиной по выбору вариативной части блока 1 учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Вычислительные сети».

Требования к результатам освоения

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

– способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты (ПК-4)
– способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений (ПК-7)
– способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации (ПК-13)
– способностью оценивать угрозы безопасности информации в компьютерных сетях (ПС-7)

Содержание дисциплины

Раздел 1. Дизайн внутренней маршрутизации для корпоративных сетей
Протоколы OSPF, EIGRP, IS-IS. Дизайн и настройка протоколов динамической маршрутизации.
Раздел 2. Дизайн BGP-маршрутизации для корпоративных сетей
Протокол BGP, настройка, дизайн протокола. Атрибуты протокола BGP.
Раздел 3. Корпоративная WAN связь
MPLS – основные понятия технологии мультипротокольной коммутации по меткам.
Раздел 4. Интеграция корпоративного ЦОД
Дизайн центра обработки данных (ЦОД).
Раздел 5. Обеспечение безопасности служб в корпоративной сети
Службы в корпоративной сети. Организация защиты информации в корпоративных сетях.
Раздел 6. Настройка QoS для оптимизированных пользовательских возможностей
QoS – качество обслуживания в современных сетях. Настройка, механизмы качества обслуживания.
Раздел 7. Корпоративный переход на IPv6
Протокол IPv6. Планирование, дизайн, адресация IPv6.
Раздел 8. Корпоративная сеть многоадресной передачи (Multicast Network)
Многоадресная передача в корпоративной сети. Multicast Network.

Общая трудоемкость дисциплины

180 час(ов), 5 ЗЕТ

Форма промежуточной аттестации

Экзамен. Курсовой проект

Б1.В.ДВ.02.02 Разработка дизайна сети предприятия

Цели освоения дисциплины

Целью преподавания дисциплины «Разработка дизайна сети предприятия» является:

Целью преподавания дисциплины 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 «Разработка дизайна сети предприятия» Б1.В.ДВ.02.08 является дисциплиной по выбору вариативной части блока 1 учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Безопасность компьютерных сетей».

Требования к результатам освоения

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

– способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты (ПК-4)
– способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений (ПК-7)
– способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации (ПК-13)
– способностью оценивать угрозы безопасности информации в компьютерных сетях (ПС-7)

Содержание дисциплины

Раздел 1. Введение
Предмет и основные задачи дисциплины «Разработка дизайна сети предприятия», её значение в системе подготовке бакалавров по направлению «Инфокоммуникационные технологии и системы связи».
Раздел 2. Средства обеспечения безопасности инфраструктуры..
Рассмотрение средств обеспечения безопасности инфраструктуры. Листы доступа. Конфигурация различных типов листов доступа для коммутаторов. Технологии защиты коммутаторов от атак: DHCP Snooping, ARP Snooping, IP Source Guard. Протокол 802.1x и его компоненты. Протокол EAP, виды аутентификации пользователей посредством протокола EAP.

Раздел 3. 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-based policy firewall) на 2-4 уровнях модели OSI. Понятие зоны безопасности. Настройка политик межсетевого экрана. Настройка фильтрации продвинутого межсетевого экрана на 5-7 уровнях модели OSI.
Раздел 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 Cisco Easy VPN. Дизайн, поиск и устранение неисправностей в сетях удаленного доступа.

Общая трудоемкость дисциплины

180 час(ов), 5 ЗЕТ

Форма промежуточной аттестации

Экзамен. Курсовой проект

Б1.В.ДВ.03.01 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.02.03 является дисциплиной по выбору вариативной части блока 1 учебного плана

подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Криптографические методы защиты информации».

Требования к результатам освоения

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

– способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1)
– способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации (ПК-5)
– способностью принимать участие в проведении экспериментальных исследований системы защиты информации (ПК-12)

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.03.02 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.02.07 является дисциплиной по выбору вариативной части блока 1 учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». 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:

– способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1)
– способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации (ПК-5)
– способностью принимать участие в проведении экспериментальных исследований системы защиты информации (ПК-12)

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.04.01 Безопасность компьютерных сетей

Цели освоения дисциплины

Целью преподавания дисциплины «Безопасность компьютерных сетей» является:
изучение основных принципов обеспечения информационной безопасности сети.

Место дисциплины в структуре ОП

Дисциплина «Безопасность компьютерных сетей» Б1.В.ДВ.02.02 является дисциплиной по выбору вариативной части блока 1 учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Безопасность IP телефонии».

Требования к результатам освоения

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

– способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1)
– способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации (ПК-6)
– способностью настраивать правила фильтрации пакетов в компьютерных сетях (ПС-8)
– способностью конфигурировать и контролировать корректность настройки программно-аппаратных средств защиты информации в компьютерных сетях (ПС-10)

Содержание дисциплины

Раздел 1. Угрозы сетевой безопасности в современном мире
Угрозы сети, уязвимости, виды угроз.
Раздел 2. Защита сетевых устройств
Управление и мониторинг устройств, Распределение доступа по привилегиям, защита плоскости управления.

Раздел 3. Авторизация, аутентификация и учет доступа (AAA).
Протокол AAA, локальная аутентификация, серверная аутентификация (протоколы RADIUS, DIAMETER)
Раздел 4. Реализация технологий брендмауера
Листы контроля доступа, межсетевые экраны, фаервол на основе зон.
Раздел 5. Внедрение системы защиты от вторжений (IPS)
Технологии IPS, сигнатуры, внедрение IPS.
Раздел 6. Обеспечение безопасности для локальной сети (LAN)
Защита коммутаторов, port-security, защита конечных устройств
Раздел 7. Криптографические системы. Внедрение виртуальных частных сетей (VPN).
Основные алгоритмы криптографии применительно к локальным вычислительным сетям. Протокол IPSEC, виртуальные частные сети.
Раздел 8. Управление безопасной сетью. ASA устройства безопасности.
Фаерволы Cisco ASA, конфигурирование, доступ, поиск неисправностей.
Раздел 9. Управление безопасностью сети
Управление сетевой безопасностью. Разработка концепции безопасности сети.

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

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.02.06 является дисциплиной по выбору вариативной части блока 1 учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». 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:

– способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1)
– способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации (ПК-6)
– способностью настраивать правила фильтрации пакетов в компьютерных сетях (ПС-8)
– способностью конфигурировать и контролировать корректность настройки программно-аппаратных средств защиты информации в компьютерных сетях (ПС-10)

Содержание дисциплины

Раздел 1. Введение
Предмет и основные задачи дисциплины «Защита информации с помощью маршрутизаторов и коммутаторов», её значение в сис¬теме подготовке бакалавров по направлению «Инфокоммуникационные технологии и системы связи».
Раздел 2. Средства обеспечения безопасности инфраструктуры..
Рассмотрение средств обеспечения безопасности инфраструктуры. Листы доступа. Конфигурация различных типов листов доступа для коммутаторов. Технологии защиты коммутаторов от атак: DHCP Snooping, ARP Snooping, IP Source Guard. Протокол 802.1x и его компоненты. Протокол EAP, виды аутентификации пользователей посредством протокола EAP.
Раздел 3. 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-based policy firewall) на 2-4 уровнях модели OSI. Понятие зоны безопасности. Настройка политик межсетевого экрана. Настройка фильтрации продвинутого межсетевого экрана на 5-7 уровнях модели OSI.
Раздел 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 Cisco Easy VPN. Дизайн, поиск и устранение неисправностей в сетях удаленного доступа.

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

Б1.В.ДВ.05.01 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.ДВ.01.03 является дисциплиной по выбору вариативной части блока 1 учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Защищенные операционные системы».

Требования к результатам освоения

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

– способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2)

– способностью проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах (ПС-6)
– способностью анализировать функционирование программного обеспечения с целью определения возможного вредоносного воздействия (ПС-15)

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.ДВ.05.02 Уязвимости программного обеспечения

Цели освоения дисциплины

Целью преподавания дисциплины «Уязвимости 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 «Уязвимости программного обеспечения» Б1.В.ДВ.01.06 является дисциплиной по выбору вариативной части блока 1 учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Алгоритмизация и программирование».

Требования к результатам освоения

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

– способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2)
– способностью проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах (ПС-6)
– способностью анализировать функционирование программного обеспечения с целью определения возможного вредоносного воздействия (ПС-15)

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.ДВ.06.01 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.

Место дисциплины в структуре ОП

Дисциплина «Программы для ЭВМ и базы данных как объекты интеллектуальной собственности» Б1.В.ДВ.01.02 является дисциплиной по выбору вариативной части блока 1 учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». 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:

– способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов (ПК-8)
– способностью осуществлять мероприятия по противодействию угрозам безопасности информации, возникающим при эксплуатации программного обеспечения (ПС-16)
– способностью анализировать эффективность сформулированных требований к встроенным средствам защиты информации программного обеспечения (ПС-18)

Содержание дисциплины

Раздел 1. формирование фундамента подготовки будущих специалистов в области инфокоммуникаций
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. Курсовая работа

Б1.В.ДВ.06.02 Лицензирование программного обеспечения

Цели освоения дисциплины

Целью преподавания дисциплины «Лицензирование программного обеспечения» является:
изучение вопросов лицензирования программного обеспечения в телекоммуникационных системах

Место дисциплины в структуре ОП

Дисциплина «Лицензирование программного обеспечения» Б1.В.ДВ.01.05 является дисциплиной по выбору вариативной части блока 1 учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Документоведение».

Требования к результатам освоения

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

– способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов (ПК-8)
– способностью осуществлять мероприятия по противодействию угрозам безопасности информации, возникающим при эксплуатации программного обеспечения (ПС-16)
– способностью анализировать эффективность сформулированных требований к встроенным средствам защиты информации программного обеспечения (ПС-18)

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. Тенденция развития лицензирования ПО
Скорость развития лицензирования ПО и рассмотр того с чем это связано

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет. Курсовая работа

Б1.В.ДВ.07.01 Защита операционных систем сетевых устройств

Цели освоения дисциплины

Целью преподавания дисциплины «Защита операционных систем сетевых устройств» является:
Целью преподавания дисциплины является изучение вопросов защиты операционных систем.

Место дисциплины в структуре ОП

Дисциплина «Защита операционных систем сетевых устройств» Б1.В.ДВ.03.01 является дисциплиной по выбору вариативной части блока 1 учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». 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:

– способностью администрировать подсистемы информационной безопасности объекта защиты (ПК-3)
– способностью оценивать угрозы безопасности информации операционных систем (ПС-2)
– способностью выбирать режимы работы программно-аппаратных средств защиты информации в операционных системах (ПС-4)

Содержание дисциплины

Раздел 1. История развития операционных систем
История разработки ОС MSDOS, Windowsи Unix.Версии ОС. Стандарт POSIX. Развитие проекта GNU, лицензия GNUGPL. Создание и развития дистрибутивов GNU/Linux. Анализ достоинств и недостатков различных операционных систем.
Раздел 2. Основы взаимодействия с ОС GNULinux.
Сеанс работы пользователя в ОС: от регистрации в системе до выхода. Даются основы работы с интерфейсами командной строки и GUI. Основные понятия файловой системы:

файл, каталог, дерево каталогов. Обсуждаются принципы размещения файлов в соответствии со стандартом FHS, приводится краткий обзор стандартных каталогов файловой системы EXT. Создание «песочницы» в ОС GNULinuxдля ограничений доступа к сервисам. Ведение системного журнала.
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

180 час(ов), 5 ЗЕТ

Форма промежуточной аттестации

Экзамен

Б1.В.ДВ.07.02 Операционные системы

Цели освоения дисциплины

Целью преподавания дисциплины «Операционные системы» является: изучение вопросов защиты операционных систем.

Место дисциплины в структуре ОП

Дисциплина «Операционные системы» Б1.В.ДВ.03.03 является дисциплиной по выбору вариативной части блока 1 учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Безопасность Astra Linux».

Требования к результатам освоения

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

– способностью администрировать подсистемы информационной безопасности объекта защиты (ПК-3)
– способностью оценивать угрозы безопасности информации операционных систем (ПС-2)
– способностью выбирать режимы работы программно-аппаратных средств защиты информации в операционных системах (ПС-4)

Содержание дисциплины

Раздел 1. История развития операционных систем
История разработки ОС MSDOS, Windowsи Unix.Версии ОС. Стандарт POSIX. Развитие проекта GNU, лицензия GNUGPL. Создание и развития дистрибутивов GNU/Linux. Анализ достоинств и недостатков различных операционных систем.
Раздел 2. Основы взаимодействия с ОС GNULinux.
Сеанс работы пользователя в ОС: от регистрации в системе до выхода. Даются основы работы с интерфейсами командной строки и GUI. Основные понятия файловой системы: файл, каталог, дерево каталогов. Обсуждаются принципы размещения файлов в соответствии со стандартом FHS, приводится краткий обзор стандартных каталогов файловой системы EXT. Создание «песочницы» в ОС GNULinuxдля ограничений доступа к сервисам. Ведение системного журнала.
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

180 час(ов), 5 ЗЕТ

Форма промежуточной аттестации

Экзамен

Б1.В.ДВ.08.01 Безопасность IP телефонии

Цели освоения дисциплины

Целью преподавания дисциплины «Безопасность IP телефонии» является: 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 вариативной части блока 1 учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Безопасность компьютерных сетей».

Требования к результатам освоения

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

– способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1)
– способностью конфигурировать и контролировать корректность настройки программно-аппаратных средств защиты информации в компьютерных сетях (ПС-10)

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 VoIP-сетях. 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.08.02 Защита голосового трафика в сети Интернет

Цели освоения дисциплины

Целью преподавания дисциплины «Защита голосового 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 голосового трафика в сети Интернет» Б1.В.ДВ.02.05 является дисциплиной по выбору вариативной части блока 1 учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». 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:

– способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1)
– способностью конфигурировать и контролировать корректность настройки программно-аппаратных средств защиты информации в компьютерных сетях (ПС-10)

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 VoIP-сетях. 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.09.01 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.ДВ.01.01 является дисциплиной по выбору вариативной части блока 1 учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Цифровая криминалистика».

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)
– способностью принимать участие в проведении экспериментальных исследований системы защиты информации (ПК-12)
– способностью анализировать угрозы безопасности информации программного обеспечения (ПС-13)

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. Курсовая работа

Б1.В.ДВ.09.02 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.01.04 является дисциплиной по выбору вариативной части блока 1 учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». 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:

– способностью принимать участие в проведении экспериментальных исследований системы защиты информации (ПК-12)
– способностью выбирать режимы работы программно-аппаратных средств защиты информации в компьютерных сетях (ПС-11)
– способностью анализировать угрозы безопасности информации программного обеспечения (ПС-13)

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 ключами
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. Курсовая работа

Б1.В.ДВ.10.01 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.04.01 является дисциплиной по выбору вариативной части блока 1 учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». 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:

– способностью использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности (ОК-9)

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.10.02 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.04.02 является дисциплиной по выбору вариативной части блока 1 учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». 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:

– способностью использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности (ОК-9)

Содержание дисциплины

Раздел 1. Методика проведения учебно-тренировочного занятия.
Оценка двигательной активности и суточных энергетических затрат. Базовый комплекс упражнений общей физической подготовки.
Раздел 2. Овладение методами и способами физкультурно-спортивной деятельности.
Методика проведения производственной гимнастики с учетом заданных условий и характера труда. Базовый комплекс упражнений общей физической подготовки. Методы тренировки. Совершенствование координационных способностей.
Раздел 3. Развитие основных физических качеств с учетом противопоказаний при различных заболеваниях.
Методы самоконтроля здоровья, физического развития и функциональной подготовленности. Круговая тренировка. Упражнения для развития выносливости (адаптивные формы): силовые упражнения с постепенным увеличением времени их выполнения; беговые упражнения на различные дистанции с различными интервалами отдыха (анаэробная и аэробная нагрузка).
Раздел 4. Повышение уровня функциональных и двигательных способностей, направленного формирования качеств и свойств личности.
Методика самооценки уровня и динамики физической подготовленности. Комплексное занятие: упражнения для развития гибкости, выносливости (адаптивные формы), силы (адаптивные формы), быстроты и ловкости.
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. Использование подвижных, спортивных игр.
Раздел 6. Приобретение опыта практической деятельности, повышение уровня функциональных и двигательных способностей.
Комплексное занятие: упражнения для развития гибкости, выносливости (адаптивные формы), силы (адаптивные формы), быстроты и ловкости. Использование гимнастических упражнений, элементов аэробики (адаптивные формы).

Общая трудоемкость дисциплины

328 час(ов),

Форма промежуточной аттестации

Зачет

Б1.В.ДВ.10.03 Секции по видам спорта

Цели освоения дисциплины

Целью преподавания дисциплины «Секции по видам спорта» является:

Целью преподавания дисциплины «Элективные дисциплины по физической культуре и спорту (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.10.03 является дисциплиной по выбору вариативной части блока 1 учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». 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:

– способностью использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности (ОК-9)

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. Ознакомление и обучение двигательным навыкам, техническими приемами в избранном виде спорта. Комплексное занятие: упражнения для развития основных физических качеств.
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

3. Аннотации программ практик

учебной Б2.В.01.01(У) Практика по получению первичных профессиональных умений и навыков

Цели проведения практики

Целью проведения практики «Практика по получению первичных профессиональных умений и навыков» 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

«Практика по получению первичных профессиональных умений и навыков» Б2.В.01.01(У) входит в блок 2 учебного плана, который относится к вариативной части, и является обязательной составной частью образовательной программы по направлению «10.03.01 Информационная безопасность».

«Практика по получению первичных профессиональных умений и навыков» опирается на знания полученные при изучении предшествующих дисциплин.

Требования к результатам освоения

В процессе прохождения практики студент формирует и демонстрирует следующие компетенции:

– способностью использовать нормативные правовые акты в профессиональной деятельности (ОПК-5)
– способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7)
– способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1)
– способностью администрировать подсистемы информационной безопасности объекта защиты (ПК-3)
– способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов (ПК-8)
– способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности (ПК-9)

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.В.02.01(П) Проектно-технологическая практика

Цели проведения практики

Целью проведения практики «Проектно-технологическая 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

«Проектно-технологическая практика» Б2.В.02.01(П) входит в блок 2 учебного плана, который относится к вариативной части, и является обязательной составной частью образовательной программы по направлению «10.03.01 Информационная безопасность».

«Проектно-технологическая практика» опирается на знания полученные при изучении предшествующих дисциплин, а также на знания и практические навыки, полученные при прохождении практик(и) «Практика по получению первичных профессиональных умений и навыков».

Требования к результатам освоения

В процессе прохождения практики студент формирует и демонстрирует следующие компетенции:

– способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1)
– способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2)
– способностью администрировать подсистемы информационной безопасности объекта защиты (ПК-3)
– способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты (ПК-4)
– способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации (ПК-5)
– способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации (ПК-6)
– способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений (ПК-7)
– способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов (ПК-8)
– способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности (ПК-9)
– способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-10)
– способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов (ПК-11)
– способностью принимать участие в проведении экспериментальных исследований системы защиты информации (ПК-12)
– способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации (ПК-13)
– способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности (ПК-14)
– способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю (ПК-15)
– способностью формулировать и настраивать политики безопасности операционных систем (ПС-1)
– способностью оценивать угрозы безопасности информации операционных систем (ПС-2)
– способностью противодействовать угрозам безопасности информации с использованием встроенных средств защиты информации операционных систем (ПС-3)
– способностью выбирать режимы работы программно-аппаратных средств защиты информации в операционных системах (ПС-4)
– способностью устанавливать и настраивать антивирусные средства защиты информации в операционных системах (ПС-5)
– способностью проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах (ПС-6)

– способностью оценивать угрозы безопасности информации в компьютерных сетях (ПС-7)
– способностью настраивать правила фильтрации пакетов в компьютерных сетях (ПС-8)
– способностью обосновывать выбор используемых программно-аппаратных средств защиты информации в компьютерных сетях (ПС-9)
– способностью конфигурировать и контролировать корректность настройки программно-аппаратных средств защиты информации в компьютерных сетях (ПС-10)
– способностью выбирать режимы работы программно-аппаратных средств защиты информации в компьютерных сетях (ПС-11)
– способностью проводить мониторинг функционирования программно-аппаратных средств защиты информации в компьютерных сетях (ПС-12)
– способностью анализировать угрозы безопасности информации программного обеспечения (ПС-13)
– способностью формулировать и обосновывать правила безопасной эксплуатации программного обеспечения (ПС-14)
– способностью анализировать функционирование программного обеспечения с целью определения возможного вредоносного воздействия (ПС-15)
– способностью осуществлять мероприятия по противодействию угрозам безопасности информации, возникающим при эксплуатации программного обеспечения (ПС-16)
– способностью определять порядок функционирования программного обеспечения с целью обеспечения защиты информации (ПС-17)
– способностью анализировать эффективность сформулированных требований к встроенным средствам защиты информации программного обеспечения (ПС-18)

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.02.02(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).

- Изучить документацию к средствам защиты, использующимся на территории РФ- Изучить основы организации систем контроля доступа и видеонаблюдения на режимном объекте - Изучить основные механизмы защиты в телекоммуникационных сетях

Место практики в структуре ОП

«Преддипломная практика» Б2.В.02.02(Пд) входит в блок 2 учебного плана, который относится к вариативной части, и является обязательной составной частью образовательной программы по направлению «10.03.01 Информационная безопасность».

«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:

– способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации (ОПК-4)
– способностью использовать нормативные правовые акты в профессиональной деятельности (ОПК-5)

– способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7)
– способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1)
– способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2)
– способностью администрировать подсистемы информационной безопасности объекта защиты (ПК-3)
– способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты (ПК-4)
– способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации (ПК-5)
– способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации (ПК-6)
– способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений (ПК-7)
– способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов (ПК-8)
– способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности (ПК-9)
– способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-10)
– способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов (ПК-11)
– способностью принимать участие в проведении экспериментальных исследований системы защиты информации (ПК-12)

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

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) «10.03.01 Информационная безопасность», ориентированной на на следующие виды деятельности:
- эксплуатационная
- проектно-технологическая
- экспериментально-исследовательская
- организационно-управленческая.

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:

– способностью использовать основы философских знаний для формирования мировоззренческой позиции (ОК-1)
– способностью использовать основы экономических знаний в различных сферах деятельности (ОК-2)

– способностью анализировать основные этапы и закономерности исторического развития России, ее место и роль в современном мире для формирования гражданской позиции и развития патриотизма (ОК-3)
– способностью использовать основы правовых знаний в различных сферах деятельности (ОК-4)
– способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики (ОК-5)
– способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия (ОК-6)
– способностью к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности (ОК-7)
– способностью к самоорганизации и самообразованию (ОК-8)
– способностью использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности (ОК-9)
– способностью анализировать физические явления и процессы для решения профессиональных задач (ОПК-1)
– способностью применять соответствующий математический аппарат для решения профессиональных задач (ОПК-2)
– способностью применять положения электротехники, электроники и схемотехники для решения профессиональных задач (ОПК-3)
– способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации (ОПК-4)
– способностью использовать нормативные правовые акты в профессиональной деятельности (ОПК-5)
– способностью применять приемы оказания первой помощи, методы и средства защиты персонала предприятия и населения в условиях чрезвычайных ситуаций, организовать мероприятия по охране труда и технике безопасности (ОПК-6)
– способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7)
– способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1)
– способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2)
– способностью администрировать подсистемы информационной безопасности объекта защиты (ПК-3)
– способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты (ПК-4)
– способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации (ПК-5)
– способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации (ПК-6)
– способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений (ПК-7)
– способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов (ПК-8)

– способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности (ПК-9)
– способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-10)
– способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов (ПК-11)
– способностью принимать участие в проведении экспериментальных исследований системы защиты информации (ПК-12)
– способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации (ПК-13)
– способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности (ПК-14)
– способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю (ПК-15)
– способностью формулировать и настраивать политики безопасности операционных систем (ПС-1)
– способностью оценивать угрозы безопасности информации операционных систем (ПС-2)
– способностью противодействовать угрозам безопасности информации с использованием встроенных средств защиты информации операционных систем (ПС-3)
– способностью выбирать режимы работы программно-аппаратных средств защиты информации в операционных системах (ПС-4)
– способностью устанавливать и настраивать антивирусные средства защиты информации в операционных системах (ПС-5)
– способностью проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах (ПС-6)
– способностью оценивать угрозы безопасности информации в компьютерных сетях (ПС-7)
– способностью настраивать правила фильтрации пакетов в компьютерных сетях (ПС-8)
– способностью обосновывать выбор используемых программно-аппаратных средств защиты информации в компьютерных сетях (ПС-9)
– способностью конфигурировать и контролировать корректность настройки программно-аппаратных средств защиты информации в компьютерных сетях (ПС-10)
– способностью выбирать режимы работы программно-аппаратных средств защиты информации в компьютерных сетях (ПС-11)
– способностью проводить мониторинг функционирования программно-аппаратных средств защиты информации в компьютерных сетях (ПС-12)
– способностью анализировать угрозы безопасности информации программного обеспечения (ПС-13)
– способностью формулировать и обосновывать правила безопасной эксплуатации программного обеспечения (ПС-14)
– способностью анализировать функционирование программного обеспечения с целью определения возможного вредоносного воздействия (ПС-15)
– способностью осуществлять мероприятия по противодействию угрозам безопасности информации, возникающим при эксплуатации программного обеспечения (ПС-16)
– способностью определять порядок функционирования программного обеспечения с целью обеспечения защиты информации (ПС-17)
– способностью анализировать эффективность сформулированных требований к встроенным средствам защиты информации программного обеспечения (ПС-18)

Содержание
Подготовка и защита выпускной квалификационной работы
Общая трудоемкость дисциплины 216 час(ов), 6 ЗЕТ