

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

---

УТВЕРЖДАЮ  
Декан ИКСС

Д.В. Окунева

**СБОРНИК АННОТАЦИЙ**

рабочих программ дисциплин

образовательной программы высшего образования

Направление подготовки «10.03.01 Информационная безопасность»,

направленность профиль образовательной программы

«Техническая защита информации»

Санкт-Петербург

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

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

Цели освоения дисциплины

---

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

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

---

Место дисциплины в структуре ОП

---

Дисциплина «История (история России, всеобщая история)» Б1.О.01 является дисциплиной обязательной части учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Изучение дисциплины «История (история России, всеобщая история)» основывается на базе знаний, умений и компетенций, полученных студентами в ходе освоения школьных курсов.

---

Требования к результатам освоения

---

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

- Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма (ОПК-13)
  - Способен воспринимать межкультурное разнообразие общества в социально-историческом, этическом и философском контекстах (УК-5)
- 

Содержание дисциплины

---

#### Раздел 1. Введение в историю

Теория и методология исторической науки. История как наука: предмет, цели, задачи изучения. Сущность, формы и функции исторического знания. Исторический источник: понятие и классификация. Виды источников. Методология истории. Историография истории. История России как неотъемлемая часть всемирной истории. Великое переселение народов. Восточные славяне в древности: теории этногенеза славян; историко-географические аспекты формирования восточных славян. Общественно-политический строй, экономика и верования восточных славян

#### Раздел 2. Русские земли и средневековый мир (V - XV вв.)

Средневековье как этап всемирной истории. Периодизация и региональная специфика средневековья. От Древней Руси к Московскому государству (IX- XV вв.). Древнерусское

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

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

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

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

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

Раздел 5. Россия и мир в XX - начале XXI в.

Великая российская революция: 1917-1922. Февраль 1917 г. и его итоги. Октябрь 1917 г. Россия в годы Гражданской войны и интервенции. Образование СССР. Советская модернизация: основные этапы и направления. Внешняя политика (1920-е1940- е гг.). Новая экономическая политика (НЭП). Советская политическая система и ее особенности. Советская внешняя политика в межвоенное десятилетие. СССР во второй мировой и Великой Отечественной войнах. Антигитлеровская коалиция. Итоги войны. Россия и мир во второй половине XX в. «Холодная война». СССР в послевоенный период (1945-1985). «Перестройка». Внешняя политика. Нарастание центробежных сил и распад СССР. Постсоветская Россия и мир (конец XX- начало XXI вв.). Крушение биполярного мира и его последствия. Российская Федерация: 1991-1999. Российская Федерация на современном этапе. Культура современной России

---

Общая трудоемкость дисциплины

144 час(ов), 4 ЗЕТ

Форма промежуточной аттестации

Экзамен

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

Цели освоения дисциплины

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

Место дисциплины в структуре ОП

Дисциплина «Физическая культура и спорт» Б1.О.02 является дисциплиной обязательной части учебного плана подготовки 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:

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

Содержание дисциплины

Раздел 1. Физическая культура в профессиональной подготовке студентов и спортивная подготовка студентов в образовательном процессе.

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

Раздел 2. Базовый комплекс занятий по общей физической подготовке.  
Упражнения для развития основных физических качеств. Совершенствование координационных способностей.

Раздел 3. Комплекс занятий по общей физической подготовке.  
Упражнения для развития выносливости, силы, ловкости, быстроты, гибкости.  
Использование подвижных, спортивных игр.

---

Общая трудоемкость дисциплины

72 час(ов), 2 ЗЕТ

Форма промежуточной аттестации

Зачет

### **Б1.О.03 Иностранный язык**

---

Цели освоения дисциплины

Целью преподавания дисциплины «Иностранный язык» является: повышение 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:

– Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(ых) языке(ах) (УК-4)

---

Содержание дисциплины

### Раздел 1. Социально-культурная сфера общения

Язык как средство межкультурного общения. О себе. Стили общения. О городе. Родной город, Санкт-Петербург, Лондон, Вашингтон. Ориентирование в городе. Фонетика. Лексика. Грамматический строй. Диалогическая и монологическая речь в основных ситуациях. Чтение и перевод текстов.

### Раздел 2. Учебно-познавательная сфера общения

Высшее образование в России и за рубежом. СПбГУТ. Студенческая жизнь. Международные программы обмена для студентов. Техническое образование в России и за рубежом. Роль иностранного языка в современном мире. Фонетика. Лексика. Грамматический строй. Диалогическая и монологическая речь в основных ситуациях. Чтение и перевод текстов. Деловая переписка. Деловой стиль общения. Анкета, мотивационное письмо, резюме, электронное письмо.

### Раздел 3. Профессиональная сфера общения

Профессии в сфере информационных технологий и телекоммуникаций. Деловой стиль общения. Интервью о приеме на работу. Деловая переписка. Составление служебных записок. Фонетика. Лексика. Грамматический строй. Диалогическая и монологическая речь в основных ситуациях. Чтение и перевод текстов.

### Раздел 4. Профессиональная сфера общения (продолжение)

Информационные технологии. Научно-технический прогресс и его достижения в сфере инфокоммуникационных технологий и систем связи. Виды сетей связи. Средства связи. Информационная безопасность. Деловой стиль общения. Деловая переписка. Различные виды документов. Виды делового письма и правила его оформления. Фонетика. Лексика. Грамматический строй. Диалогическая и монологическая речь в основных ситуациях. Чтение и перевод текстов.

Общая трудоемкость дисциплины

360 час(ов), 10 ЗЕТ

Форма промежуточной аттестации

Экзамен

## **Б1.О.04 Экономика**

Цели освоения дисциплины

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

Место дисциплины в структуре ОП

Дисциплина «Экономика» Б1.Б.05 является 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:

- Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений; (ОПК-12)
- Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений (УК-2)
- Способен принимать обоснованные экономические решения в различных областях жизнедеятельности (УК-9)

---

#### Содержание дисциплины

---

##### Раздел 1. Введение в экономическую науку

Краткий обзор этапов развития экономической мысли. Предмет и метод экономической мысли. Предмет и метод экономической теории. Базовые экономические понятия. Экономические системы. Институциональные основы функционирования рынка.

##### Раздел 2. Спрос, предложение и рыночное равновесие

Спрос и его факторы. Предложение и его факторы. Рыночное равновесие и его устойчивость. Государственное регулирование индивидуальных рынков.

##### Раздел 3. Эластичность спроса и предложения

Эластичность спроса по цене. Факторы ценовой эластичности спроса. Взаимосвязь ценовой эластичности спроса и общей выручки продавцов. Эластичность спроса по доходу. Перекрестная эластичность спроса. Эластичность предложения.

##### Раздел 4. Издержки производства. Фирма в условиях совершенной конкуренции

Фирма. Экономические и бухгалтерские издержки фирмы. Постоянные, переменные, общие, средние и предельные издержки фирмы. Издержки в длительном периоде. Совершенная и несовершенная конкуренция. Правило максимизации прибыли фирмы. Точка безубыточности, точка закрытия и кривая предложения конкурентной фирмы.

##### Раздел 5. Фирма в условиях несовершенной конкуренции

Монополия. Максимизация прибыли монополий. Ценовая дискриминация. Ущерб, наносимый монополией обществу. Государственная антимонопольная политика. Олигополия. Модели олигополии: ценовая война, ломаная кривая спроса, картель, лидерство в ценах. Монополистическая конкуренция. Равновесие фирмы на рынке монополистической конкуренции в краткосрочном и долгосрочном периодах.

##### Раздел 6. Основные макроэкономические показатели. Модель общего экономического равновесия

Валовый внутренний продукт (ВВП) и принципы его расчета. Валовый национальный продукт, чистый национальный продукт, национальный доход, личный доход, личный располагаемый доход. Дефлятор ВВП и Индекс потребительских цен.

Макроэкономическая производственная функция. Функция потребления, инвестиционная функция. Роль ставки ссудного процента в установлении равновесия. Равновесие на финансовых рынках. Эффект вытеснения.

#### Раздел 7. Макроэкономическая нестабильность: инфляция и безработица

Сущность, функции и виды денег. Количественная теория денег и основная причина инфляции. Сеньораж. Гиперинфляция и пути её подавления. Общественные издержки инфляции. Измерение уровня безработицы. Основные причины безработицы. Закон Оукена. Кривая Филлипса.

#### Раздел 8. Теория экономических колебаний. Модель совокупного спроса и совокупного предложения (AD-AS)

Краткосрочные и долгосрочные экономические колебания. Кривая совокупного спроса AD и её сдвиги. Краткосрочная и долгосрочная кривые совокупного предложения. Равновесие в краткосрочном и долгосрочном периодах.

#### Раздел 9. Влияние кредитно-денежной политики на совокупный спрос. Кейнсианская теория национального дохода.

Шоки со стороны совокупного спроса и совокупного предложения. Политика стабилизации. Модель кейнсианского креста. Парадокс бережливости. Модель кейнсианского креста. Парадокс бережливости.

#### Раздел 10. Налогово-бюджетная политика и мультипликатор

Мультипликатор государственных расходов, налоговый мультипликатор.

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

### **Б1.О.05 Философия**

Цели освоения дисциплины

Целью преподавания дисциплины «Философия» является: формирование философской культуры мышления, осознанного отношения к наиболее общим принципам познания и практической деятельности, способности критического анализа и совместного обсуждения идей универсального характера. Дисциплина должна обеспечить усвоение общетеоретического, мировоззренческого фундамента подготовки будущих специалистов в области технических и гуманитарных наук, создать необходимую базу для успешного овладения последующими дисциплинами учебного плана. Она должна способствовать развитию творческих способностей студентов, умению применять и самостоятельно пополнять и углублять полученные научные знания. Эти цели достигаются на основе индивидуализации процесса обучения путём использования достижений современной философской и научной мысли. В результате изучения дисциплины у студентов должны сформироваться знания, умения и навыки, позволяющие проводить самостоятельный анализ глобальных,



общечеловеческих и конкретных явлений современной жизни. Приобретенные студентами знания и навыки необходимы для формирования способности к обобщению, анализу, критическому восприятию информации любого рода, к самостоятельной постановке целей и выбору путей их достижения на основе высших ценностей жизни и культуры, а также для умения логически верно, аргументированно и ясно строить устную и письменную речь. Философские знания необходимы для понимания социально и личностно значимых проблем.

---

Место дисциплины в структуре ОП

---

Дисциплина «Философия» Б1.Б.06 является базовой дисциплиной цикла учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Изучение дисциплины «Философия» основывается на базе знаний, умений и компетенций, полученных студентами в ходе освоения школьных курсов.

---

Требования к результатам освоения

---

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

- Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач (УК-1)
  - Способен воспринимать межкультурное разнообразие общества в социально-историческом, этическом и философском контекстах (УК-5)
- 

Содержание дисциплины

---

### Раздел 1. Что есть философия?

Что есть философия? (часть 1): понятие философии, ее особое положение среди других наук. Генезис философии. Что есть философия? (часть 2): структура философии (основные философские науки). Категории, принципы и законы философии. Функции философии. Понятие мировоззрения, типы мировоззрения. Основные проблемы философии. Основные философские направления.

### Раздел 2. История философии

Философия древности: досократики, Софисты и Сократ: основание философии западной морали, Платон: основание философского идеализма, Аристотель: первая систематизация знаний, стоицизм и неоплатонизм, Философия Средневековья: патристика и схоластика, Философия эпохи Возрождения, Новоевропейская наука и метафизика, Критическая философия И.Канта, Диалектика Г.Гегеля и марксизма, Современная западная философия, Отечественная философия

### Раздел 3. Философия бытия

Развитие понятия бытия (от Парменида до Гегеля). Понятие материи и его развитие от античного материализма до марксизма. Понятия движения, пространства и времени. Понятие идеи, его диалектика и математические начала онтологии

---

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

---

### ***Б1.0.06 Безопасность жизнедеятельности***

---

Цели освоения дисциплины

---

Целью преподавания дисциплины «Безопасность жизнедеятельности» является:

формирование профессиональной культуры безопасности, предполагающей готовность и способность выпускника использовать приобретенную совокупность знаний, умений и навыков для обеспечения безопасности в сфере профессиональной деятельности и в условиях чрезвычайных ситуаций.

---

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:

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

---

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 поражающие 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

72 час(ов), 2 ЗЕТ

Форма промежуточной аттестации

Зачет

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

Цели освоения дисциплины

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

Место дисциплины в структуре ОП

Дисциплина «Математический анализ» Б1.О.07.01 является дисциплиной обязательной части учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Изучение дисциплины «Математический анализ» основывается на базе знаний, умений и компетенций, полученных студентами в ходе освоения школьных курсов.

Требования к результатам освоения

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

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

Содержание дисциплины

### Раздел 1. Дифференциальное исчисление функции одной переменной

Функция. Предел. Сравнение бесконечно малых. Непрерывность функции в точке и на отрезке. Классификация точек разрыва. Понятие производной. Теоремы о среднем. Правило Лопиталя. Производные высших порядков. Исследование функции одной переменной.

### Раздел 2. Интегральное исчисление функции одной переменной

Понятие первообразной. Техника интегрирования. Задачи, решаемые с помощью определённого интеграла. Свойства определённого интеграла. Несобственный интеграл. Понятие сходимости.

### Раздел 3. Функции многих переменных.

Частные производные. Особенности исследования функции многих переменных. Производная по направлению и градиент. Дивергенция и ротор

### Раздел 4. Кратные интегралы

Двойной интеграл, понятие и приложения. Вычисление двойного интеграла в декартовых и полярных координатах. Понятие о тройном интеграле.

### Раздел 5. Криволинейные интегралы.

Криволинейные интегралы первого и второго типов. Условие независимости криволинейного интеграла от пути интегрирования. Формула Грина. Вычисление

криволинейных и поверхностных интегралов непосредственно и с использованием формул Остроградского –Гаусса и Стокса.

#### Раздел 6. Дифференциальные уравнения.

Понятие дифференциального уравнения. Постановка задачи Коши, существование и единственность решений. Методы решения дифференциальных уравнений различных типов. Основные положения теории линейных дифференциальных уравнений.

#### Раздел 7. Теория рядов.

Числовой ряд и его сумма. Признаки сходимости числовых рядов. Функциональные ряды. Степенной ряд, его свойства, операции над сходящимися степенными рядами. Ряды Тейлора и Маклорена. Тригонометрический ряд. Понятие ортонормированной системы функций. Ряды Фурье

#### Раздел 8. Интегральные преобразования.

Преобразование Фурье, свойства прямого и обратного преобразований. Оператор Лапласа, его свойства. Методы нахождения изображений и оригиналов. Решение задач операторным методом.

#### Раздел 9. Элементы теории поля

Векторное поле. Его характеристики. Понятие потока векторного поля.

---

Общая трудоемкость дисциплины

288 час(ов), 8 ЗЕТ

Форма промежуточной аттестации

Зачет, Экзамен

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

Цели освоения дисциплины

---

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

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.О.07.02 является одной из дисциплин обязательной 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 «Алгебра и геометрия»; «Математический анализ».

---

## Требования к результатам освоения

---

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

- Способен использовать необходимые математические методы для решения задач профессиональной деятельности; (ОПК-3)
  - Способен проводить эксперименты по заданной методике и обработку их результатов; (ОПК-11)
- 

## Содержание дисциплины

---

### Раздел 1. Случайные события

Основные понятия теории вероятностей. События. Вероятность события. Статистический подход к описанию случайных явлений. Непосредственное определение вероятностей. Элементы комбинаторики. Размещения, перестановки, сочетания. Алгебра событий. Аксиомы теории вероятностей. Основные теоремы теории вероятностей: теорема сложения вероятностей, теорема умножения вероятностей, формула полной вероятности, теорема гипотез (формула Байеса). Последовательность независимых испытаний. Распределение Пуассона. Локальная и интегральная теоремы Муавра-Лапласа

### Раздел 2. Случайные величины

Дискретные случайные величины. Распределение дискретной случайной величины. Непрерывные случайные величины. Плотность случайной величины. Функция распределения. Числовые характеристики случайных величин. Математическое ожидание. Моменты второго порядка. Закон равномерной плотности. Закон Пуассона. Одномерное нормальное распределение.

### Раздел 3. Многомерные случайные величины

Системы случайных величин (случайные векторы). Функция распределения. Условные законы распределения. Зависимые и независимые случайные величины. Числовые характеристики системы двух случайных величин. Корреляционный момент. Коэффициент корреляции. Нормальный закон на плоскости. Вероятность попадания в область произвольной формы.

### Раздел 4. Предельные теоремы теории вероятностей

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

### Раздел 5. Цепи Маркова

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

### Раздел 6. Математическая статистика

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

### Раздел 7. Методы изучения статистических зависимостей

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

---

Общая трудоемкость дисциплины

144 час(ов), 4 ЗЕТ

Форма промежуточной аттестации

Экзамен

---

### **Б1.О.07.03 Алгебра и геометрия**

---

Цели освоения дисциплины

Целью преподавания дисциплины «Алгебра и геометрия» является: обучение умению формулировать и решать алгебраические и геометрические в рамках задачи изучаемой специальности, умению творчески применять и самостоятельно дополнять свои знания.

---

Место дисциплины в структуре ОП

---

Дисциплина «Алгебра и геометрия» Б1.О.07.03 является дисциплиной обязательной части учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Изучение дисциплины «Алгебра и геометрия» основывается на базе знаний, умений и компетенций, полученных студентами в ходе освоения школьных курсов.

---

Требования к результатам освоения

---

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

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

---

Содержание дисциплины

---

#### Раздел 1. Комплексные числа

Действия с комплексными числами в алгебраической форме. Модуль и аргумент. Особенности применения тригонометрической и показательной форм комплексного числа. Основная теорема алгебры. Извлечение корня из комплексного числа. Обзор элементарных функций комплексного переменного.

#### Раздел 2. Алгебра матриц

Понятие матрицы. Действия с матрицами. Решение матричных уравнений. Ранг матрицы. Собственные числа

### Раздел 3. Определители

Методы вычисления определителей, их свойства. Минор.

### Раздел 4. Системы линейных алгебраических уравнений

Решение систем методом Гаусса. Теоремы Крамера. Теорема Кронекера-Капелли.

Особенности решения однородных систем

### Раздел 5. Аналитическая геометрия на плоскости и в пространстве

Линейные геометрические объекты и работа с ними. Кривые и поверхности второго порядка. Использование квадратичных форм.

### Раздел 6. Линейное пространство произвольной размерности. Линейные операторы

Понятие линейного пространства произвольной размерности. Линейный оператор и его свойства.

---

Общая трудоемкость дисциплины

180 час(ов), 5 ЗЕТ

Форма промежуточной аттестации

Экзамен

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

---

Цели освоения дисциплины

Целью преподавания дисциплины «Дискретная математика» является: формирование 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 одной из дисциплин базовой 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».

---

Требования к результатам освоения

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

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



---

## Содержание дисциплины

---

### Раздел 1. Множества и операции над ними

Множества и операции над ними. Отношения и функции. Высказывания.

### Раздел 2. Булевы функции.

Булевы функции. Нормальные формы формул. ДНФ и КНФ, СДНФ и СКНФ. Минимизация булевых функций.

### Раздел 3. Понятия о предикатах и кванторах. Полнота и замкнутость. Полные системы булевых функций.

Понятия о предикатах и кванторах. Полнота и замкнутость. Полные системы булевых функций

### Раздел 4. Комбинаторика

Размещения, перестановки, сочетания. Комбинаторные схемы. Производящие функции

### Раздел 5. Теории графов.

Основные понятия и определения теории графов. Алгоритмы поиска кратчайших путей между вершинами графа. Методы решения оптимизационных задач на графах.

### Раздел 6. Транспортные сети

Транспортные сети. Алгоритм построения максимального потока в транспортной сети

### Раздел 7. Алгоритмы.

Понятия конечных автоматов. Основы теории решеток

---

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

## ***Б1.О.07.05 Теория информации***

---

Цели освоения дисциплины

---

Целью преподавания дисциплины «Теория информации» является: изучение основных закономерностей обмена информацией на расстоянии, обработки, эффективной передачи и помехоустойчивого приёма в технических и естественных системах различного назначения и формирования фундаментальных знаний основ теории детерминированных и случайных аналоговых и цифровых сигналов и систем их преобразования, основ потенциальной помехоустойчивости и оптимального приема сигналов в каналах с помехами, принципов и методов многоканальной передачи, хранения, распределения и приема дискретных и непрерывных сообщений, аналоговых и цифровых методов модуляции, методов повышения энергетической и спектральной эффективности систем электросвязи базирующихся на фундаменте теории информации, эффективного и помехоустойчивого кодирования, способствовать развитию творческих способностей студентов, умению формулировать и решать задачи оптимизации

систем связи, умению творчески применять и самостоятельно повышать свои знания в области инфотелекоммуникаций, в том числе космической, оптической и многоканальной специальной связи..

---

Место дисциплины в структуре ОП

---

Дисциплина «Теория информации» Б1.О.07.05 является одной из дисциплин обязательной части учебного плана подготовки 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 «Алгебра и геометрия»; «Дискретная математика»; «Математический анализ»; «Теория вероятностей и математическая статистика».

---

Требования к результатам освоения

---

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

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

---

Содержание дисциплины

---

#### Раздел 1. 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.

#### Раздел 2. Математические модели случайных процессов. Прохождение случайных процессов через линейные цепи

Автокорреляционная функция случайного процесса. Применение импульсных и частотных характеристик для анализа линейных систем. Связь АКФ с энергетическим спектром случайного сигнала, теорема Винера - Хинчина, интервал корреляции, белый шум. Узкополосные случайные процессы, распределение огибающей и фазы узкополосного случайного процесса. Нормальное распределение, связь корреляции и независимости выборок из нормального случайного сигнала.

#### Раздел 3. Информационные характеристики источников сообщений и каналов. 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. энтропия (безусловная, условная), количество информации, избыточность сообщения, производительность источника. Информационные характеристики каналов: скорость передачи информации, максимальная скорость передачи информации (пропускная способность канала), коэффициент использования канала. Информационные характеристики источников дискретных сообщений. Модели источников дискретных сообщений. Свойства эргодических источников. Избыточность и производительность дискретного источника. Двоичный источник сообщений. Информационные характеристики дискретных каналов. Идеальные (без помех) и реальные (с помехами) каналы. Скорость передачи и пропускная способность канала. Двоичный и "м - ичный" канал. Информационные характеристики источников непрерывных сообщений. Дифференциальная энтропия. Энтропия равномерного распределения. Энтропия гауссовского белого шума. Эпсилон - энтропия и эпсилон — производительность источника. Избыточность. Информационные характеристики непрерывных каналов. Модели непрерывных каналов. Скорость передачи информации и пропускная способность. Сравнение пропускных способностей дискретных и непрерывных каналов.

#### Раздел 4. Основы теории передачи информации

Теоремы кодирования Шеннона для КС без помех и с помехами. Предел Шеннона. Условная энтропия источника. Эпсилон-энтропия НС.

#### Раздел 5. Основы теории эффективного кодирования дискретных Сообщений.

##### Кодирование источника ДС

Классификация кодов. Эффективное оптимальное кодирование как способ согласования информационных характеристик источника и канала. Кодирование источников без памяти (символы сообщений независимы) и с памятью (символы коррелированные между собой). Кодирование без потерь и с потерями. Кодовое дерево, префиксность кода и неравенство Крафта, 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 6. Основы теории помехоустойчивого кодирования. Кодирование канала Блочные линейные коды

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

#### Раздел 7. Сверточные коды и декодер максимального правдоподобия

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

#### Раздел 8. Основы оптимального приёма дискретных и непрерывных сообщений

Содержание и классификация задач оптимального приёма ДС. Оптимальный приём ДС в КС с детерминированной и 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 переда-точная функция согласованного фильтра.

Раздел 9. Потенциальная помехоустойчивость приёма.

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

Раздел 10. Методы многоканальной передачи и распределения информации.

Многопользовательская и многоканальная связь. Основы теории уплотнения и разделения сигналов в многоканальных системах связи. Многоканальная связь с временным, частотным, фазовым и кодовым уплотнением сигналов. Принципы создания систем инфотелекоммуникаций на основе технологии ортогонального частотного мультиплексирования. Пространственное мультиплексирование в системах ММО.

---

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

### **Б1.О.08.01 Физика**

---

Цели освоения дисциплины

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

---

Место дисциплины в структуре ОП

---

Дисциплина «Физика» Б1.Б.13.01 является базовой дисциплиной цикла учебного плана подготовки 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:

- Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности; (ОПК-4)
  - Способен проводить эксперименты по заданной методике и обработку их результатов; (ОПК-11)
- 

## Содержание дисциплины

---

### Раздел 1. Механика

Кинематика и динамика материальной точки и поступательного движения твердого тела. Работа и механическая энергия. Кинематика и динамика вращательного движения. Законы сохранения в механике. Основы специальной теории относительности

### Раздел 2. Электростатика

Электрический заряд. Закон Кулона. Электростатическое поле в вакууме. Вектор напряженности электрического поля. Силовые линии. Электростатическая теорема Гаусса. Потенциальный характер электростатического поля. Диэлектрики в электростатическом поле. Проводники в электростатическом поле. Емкость проводника и конденсатора. Энергия взаимодействия системы зарядов. Энергия заряженного конденсатора. Объемная плотность энергии электрического поля

### Раздел 3. Электрический ток

Электрический ток. Условие существования тока. Сила тока. Вектор плотности тока. Уравнение непрерывности. Закон Ома для участка цепи. Закон Ома в дифференциальной форме. Сторонние силы. Закон Ома для неоднородного участка цепи. Закон Ома для полной цепи. Закон Джоуля-Ленца в интегральной и дифференциальной формах. Работа и мощность электрического тока.

### Раздел 4. Магнитное поле

Магнитное поле. Силы, действующие в магнитном поле на движущиеся заряды и токи. Расчет магнитных полей с помощью закона Био-Савара-Лапласа. Теорема Гаусса для магнитных полей. Теорема о циркуляции магнитного поля в вакууме. Работа при перемещении витка с током в постоянном магнитном поле. Магнитные свойства вещества.

### Раздел 5. Электромагнетизм

Явление электромагнитной индукции. Закон Фарадея для электромагнитной индукции. Правило Ленца. Явление самоиндукции. Индуктивность. Токи при замыкании и размыкании цепи. Энергия магнитного поля. Объемная плотность энергии магнитного поля. Вихревое электрическое поле. Ток смещения. Система уравнений Максвелла в интегральной и дифференциальной формах

### Раздел 6. Колебания и волны

Гармонические колебания и их характеристики. Сложение гармонических колебаний. Затухающие колебания. Вынужденные колебания. Зависимость амплитуды и фазы колебаний от частоты. Резонанс. Упругие волны. Уравнение бегущей волны. Уравнение Даламбера. Плотность потока энергии, интенсивность упругой волны. Вектор Умова. Стоячие волны. Элементы акустики. Электромагнитные волны. Уравнение Даламбера для

электромагнитной волны. Свойства электромагнитных волн. Плотность потока энергии электромагнитной волны (вектор Умова - Пойнтинга).

Общая трудоемкость дисциплины

288 час(ов), 8 ЗЕТ

Форма промежуточной аттестации

Экзамен

### **Б1.О.08.02 Электротехника**

Цели освоения дисциплины

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

Место дисциплины в структуре ОП

Дисциплина «Электротехника» Б1.О.08.02 является одной из дисциплин обязательной части учебного плана подготовки 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:

- Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности; (ОПК-4)

---

## 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.О.08.03 Электроника и схемотехника**

---

Цели освоения дисциплины

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

---

Место дисциплины в структуре ОП

Дисциплина «Электроника и схемотехника» Б1.О.08.03 является одной из дисциплин обязательной части учебного плана подготовки 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:

- Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности; (ОПК-4)

---

Содержание дисциплины



---

## Раздел 1. Физические основы работы полупроводниковых приборов.

Электропроводность полупроводников. Электрические переходы. Смещение р-п-перехода. Ёмкость р-п-перехода. Пробой р-п-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 р-п-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, коэффициент 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

### **Б1.О.09.01 Информатика**

#### Цели освоения дисциплины

Целью преподавания дисциплины «Информатика» является:  
подготовка будущих специалистов по направлению специальности, владеющих теоретическими знаниями, практическими навыками применения перспективных методов, современных средств информационных технологий и умением использовать эти знания для успешного овладения последующих специальных дисциплин учебного плана; развитие творческих способностей студентов и умения решения задач различного направления

#### Место дисциплины в структуре ОП

Дисциплина «Информатика» Б1.О.09.01 является дисциплиной обязательной части 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:

- Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства; (ОПК-1)
- Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности; (ОПК-2)
- Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности; (ОПК-7)

#### Содержание дисциплины

Раздел 1. Системы счисления. Модели решения функциональных и вычислительных задач  
Системы счисления. Моделирование как метод познания. Объект, субъект, цель моделирования. Классификация моделей. Цели, задачи, решаемые с помощью моделей. Методы и технологии моделирования. Основные понятия и методы теории информации и кодирования. Сигналы, данные, информация. Общая характеристика процессов сбора, передачи, обработки и накопления информации.

## Раздел 2. . Технические средства реализации информационных процессов

Современные технические средства, построенные по принципу архитектуры ЭВМ (планшеты, мобильные устройства и т.д.)

## Раздел 3. Методы управления средствами передачи информации

Классификация, назначение операционных систем (ОС). Операционные системы: Windows, Linux и др. Особенности, отличия, интересы, области применения

## Раздел 4. Средства и методы передачи информации

Сетевые технологии обработки данных. Режимы передачи данных в компьютерных сетях. Типы синхронизации данных при передаче и способы передачи информации. Аппаратные средства, применяемые при передаче данных. Основы компьютерной коммуникации. Принципы построения и основные топологии вычислительных сетей, коммуникационное оборудование. Физическая передающая среда ЛВС и методы доступа к ней. Сетевой сервис и сетевые стандарты. Программы для работы в сети Интернет. Защита информации в локальных и глобальных компьютерных сетях. Шифрование данных. Электронная подпись.

## Раздел 5. Программные средства реализации информационных процессов

Служебные программы, утилиты. Драйверы. Архиваторы. Антивирусные программы. Встроенные программы. Прикладное программное обеспечение. ППО специального назначения. Среды программирования. Программные средства для мобильных устройств. Программные средства для периферийных устройств. ГОСТ Р ISO/МЭК 26300-2010 Информационная технология (ИТ).

---

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

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

Цели освоения дисциплины

---

Целью преподавания дисциплины «Языки программирования» является: ознакомление слушателей с основными возможностями языка программирования Python

---

Место дисциплины в структуре ОП

---

Дисциплина «Языки программирования» Б1.О.09.02 является дисциплиной обязательной части учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Изучение дисциплины «Языки программирования» основывается на базе знаний, умений и компетенций, полученных студентами в ходе освоения школьных курсов.

---

## Требования к результатам освоения

---

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

- Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства; (ОПК-1)
  - Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности; (ОПК-2)
  - Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности; (ОПК-7)
- 

## Содержание дисциплины

---

### Раздел 1. Основы Python

Введение в программирование и особенности языка

### Раздел 2. Условные выражения и циклы

Рассмотрение основных условных операторов, а также логических операторов.

### Раздел 3. Типы данных

Динамическая типизация

### Раздел 4. Функции

Создание собственных простейших функций и их вызов

### Раздел 5. Классы и объекты

Работа с простейшими классами, создание объектов

### Раздел 6. Основные свойства ооп

Рассмотрение основных свойств ООП(полиморфизм, наследование и инкапсуляция)

### Раздел 7. Использование стандартных библиотек и модулей

Рассмотрение возможности применения встроенных библиотек и модулей

### Раздел 8. Использование нестандартных библиотек и модулей

Рассмотрение возможности применения сторонних библиотек и модулей

---

Общая трудоемкость дисциплины

180 час(ов), 5 ЗЕТ

Форма промежуточной аттестации

Экзамен

---

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

Цели освоения дисциплины

---

Целью преподавания дисциплины «Технологии и методы программирования»

является:

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

---

Место дисциплины в структуре ОП

---

Дисциплина «Технологии и методы программирования» Б1.Б.14.03 является одной из дисциплин базовой 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»; «Языки программирования».

---

Требования к результатам освоения

---

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

– Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности; (ОПК-7)

---

Содержание дисциплины

---

Раздел 1. Основы объектно-ориентированного программирования.

Парадигмы программирования. Классификация языков программирования. Императивные языки программирования. Язык Си. Метод модульного программирования. Базовые понятия объектно-ориентированного программирования: объект, класс, инкапсуляция, полиморфизм, наследование. Класс в C++: сокрытие и доступность членов класса, конструктор, деструктор, перегрузка функций-членов класса, перегрузка операторов, друзья класса, использование механизма наследования, виртуальные функции. Элементы языка C++: стандартная библиотека языка C++, средства для работы с динамической памятью, консольный и файловый ввод/вывод с помощью объектов потоков.

Раздел 2. Библиотеки языка C++

Библиотеки как средство реализации метода модульного программирования. Классификация библиотек по назначению, по составу. Примеры библиотек и условия их использования. Библиотека Qt: основные классы, структура простейшего приложения с графическим интерфейсом пользователя, простейшие элементы управления, обработка приложением событий, связанных с действиями пользователя, концепция «сигнал-слот». Инструментальная среда Qt Creator для создания приложения на основе Qt.

Раздел 3. Конструирование приложения с использованием базы данных

Основные понятия теории баз данных. Модели данных. Реляционные базы данных: термины, конструирование одно- и многотабличной базу данных. Примеры реляционных СУБД. СУБД SQLite. Язык SQL: основные команды, примеры запросов на выборку.

Структура приложения, использующего базу данных. Средства организации работы приложения с базой данных. Классы Qt для взаимодействия с базой данных.

#### Раздел 4. Системы коллективной разработки программного обеспечения

Принципы организации группы разработчиков ПО. Распределение ролей в коллективе. Средства организации совместной работы. Системы контроля версий. Система Subversion: структура репозитория, основные команды управления данными, конфликты и способы их разрешения.

#### Раздел 5. Основы конструирования программных систем

Классический жизненный цикл программного обеспечения, характеристика его этапов. Стратегии конструирования ПО. Классификации ПО. Критерии качества ПО. Язык UML как средство анализа и проектирования ПО. Методы сбора и анализа требований к ПО. Концепция ПО. Спецификация и техническое задание. Средства анализа и проектирования ПО: DFD, ERD, STD, UML. Этапы проектирования. Типовые структуры ПО. Этапы и методы тестирования. Тестирование «черного ящика» и «белого ящика». Документирование программного обеспечения. Стандарты ГОСТ и ИСО в области конструирования ПО. Группа стандартов ЕСПД.

---

Общая трудоемкость дисциплины

144 час(ов), 4 ЗЕТ

Форма промежуточной аттестации

Экзамен

### **Б1.О.09.04 Документоведение**

---

Цели освоения дисциплины

Целью преподавания дисциплины «Документоведение» является:

Целью преподавания дисциплины является изучение вопросов основ построения документооборота. Дисциплина «Документоведение» должна обеспечивать формирование фундамента подготовки будущих специалистов в области инфокоммуникаций, а также, создавать необходимую базу для успешного овладения последующими специальными дисциплинами учебного плана. Она должна способствовать развитию творческих способностей студентов, умению формулировать и решать задачи изучаемой специальности, умению творчески применять и самостоятельно повышать свои знания.

---

Место дисциплины в структуре ОП

---

Дисциплина «Документоведение» Б1.О.09.04 является одной из дисциплин обязательной части учебного плана подготовки 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 «Основы информационной

безопасности».

---

## Требования к результатам освоения

---

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

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

---

## Содержание дисциплины

---

### Раздел 1. Система норм права, регулирующих деятельность телекоммуникаций в РФ

В рамках раздела изучается система норм права, регулирующих деятельность телекоммуникаций, в РФ. Субординация норм права. Конституционные основы деятельности в телекоммуникациях РФ

### Раздел 2. Система норм права, регулирующих деятельность документооборота организации в РФ

В рамках раздела изучается система норм права, регулирующих деятельность в области документооборота в РФ. Структура контрольно-надзорных органов для коммерческих и государственных организаций. Основы внутреннего и внешнего документооборота организации

### Раздел 3. Федеральная связь РФ и ее состав

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

### Раздел 4. Информация, информационные технологии, в соответствии с законом РФ "Об информации, информационных технологиях и о защите 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 ActiveDirectory в ОС WinServer.

### Раздел 8. Нормативно-правовые основы электронной подписи в ГОСТах и СНИПах.

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

#### Раздел 9. Основы DLP-систем

В рамках раздела изучаются основные понятия и 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

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

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

---

Цели освоения дисциплины

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

---

Место дисциплины в структуре ОП

---

Дисциплина «Информационные технологии» Б1.О.09.05 является одной из дисциплин обязательной части учебного плана подготовки 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».

---

Требования к результатам освоения

---

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



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

---

## Содержание дисциплины

---

### Раздел 1. Информационные технологии (ИТ)

Введение в информационные технологии, основные определения. Классификация ИТ. Информационные процессы реализации информационных технологий. Технологический процесс поиска, сбора и этапы обработки информации. Основные свойства ИТ. Методы анализ и синтеза информации.

### Раздел 2. Современные технические средства взаимодействия мобильных информационных систем

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

### Раздел 3. Информационные технологии конечного пользователя

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

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

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

### Раздел 5. Развитие информационных технологий

Искусственный интеллект (ИИ). Разновидности интеллектуальных систем (рекомендательные системы и интеллектуальные системы поддержки принятия решений.) База знаний. Онтология в ИТ. Технология распознавания. Компьютерное зрение, обработка естественного языка, распознавание и синтез речи. Современные сферы применения технологий ИИ (нейропротезирование, нейроинтерфейсы, нейростимуляция, нейросенсинг и т.п.) Квантовые технологии. Современные направления производственных технологий. Цифровое проектирование и моделирование. Технологические задачи цифрового проектирования. 3Dмоделирование в современном мире. Технология Digital Twin. Области применения цифровых двойников. Классификация «двойников». Системы PLM, MES. Компоненты робототехники и сенсорики. Сенсорика. Сенсоры, необходимые роботам. Датчики в робототехнике. Тенденции в сенсорике роботов. Технологии сенсорномоторной координации и пространственного позиционирования. Технологии пространственного позиционирования. Сенсоры и обработка сенсорной информации

### Раздел 6. Технологии и средства Интернет

Веб-технологии. URL, DNS, Типы DNSсерверов. Системы управления контентом (CMS): WordPress, Joomla, Drupal, 1С-Bitrix, MODX. Технологии SEO продвижения сайтов в поисковых системах. SEO, Метрика, Webвизор.

Общая трудоемкость дисциплины

216 час(ов), 6 ЗЕТ

Форма промежуточной аттестации

Экзамен

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

Цели освоения дисциплины

Целью преподавания дисциплины «Аппаратные средства вычислительной техники» является:

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

Место дисциплины в структуре ОП

Дисциплина «Аппаратные средства вычислительной техники» Б1.О.09.06 является одной из дисциплин обязательной части учебного плана подготовки 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:

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

Содержание дисциплины

## Раздел 1. Введение

Предмет и задачи дисциплины. История создания вычислительной техники.

## Раздел 2. Устройство персонального компьютера

Основные и дополнительные компоненты персонального компьютера.

## Раздел 3. Процессор

Назначение, устройство и принцип работы процессора. Характеристики процессора. Особенности использования процессора.

## Раздел 4. Увеличение быстродействия процессора. Система охлаждения процессора.

Методы увеличения производительности процессора. Модернизация процессора и особенности его эксплуатации. Соблюдение теплового режима. Виды теплоотводов. Причины перегрева ЦП.

## Раздел 5. Системная плата

Назначение и компоненты системной платы. Чипсет системы плат. Внутренние и внешние интерфейсы системной платы.

## Раздел 6. Оперативная память. Видеоадаптеры.

Назначение и характеристики оперативной памяти. Принципы работы оперативной памяти. Стандарты оперативной памяти. Назначение, стандарты и компоненты видеоадаптера. Интерфейсы и разъемы видеоадаптера. Принципы работы и характеристики видеоадаптера.

## Раздел 7. Звуковое обеспечение. Накопители информации

Звуковые платы. Принципы функционирования и характеристики звуковой платы. Накопители на жёстких магнитных дисках. Сменные накопители на основе flash памяти. Накопители на оптических дисках. Интерфейсы накопителей информации

## Раздел 8. Блок питания. Монитор.

Назначение, принципы работы и характеристики блока питания ПК. Выбор блока питания ПК. Назначение, типы и основные характеристики мониторов. Принципы работы СКЕ и LCD мониторов, принципы работы плазменных и OLED мониторов.

## Раздел 9. Устройства ввода информации. Клавиатура. Мышь.

Устройства ввода информации. Манипулятор типа мышь. Графический планшет.

## Раздел 10. Заключение

Перспективные направления проектирования вычислительных устройств. Вычислительные кластеры. Аппаратные средства для распределенных вычислений.

Общая трудоемкость дисциплины

180 час(ов), 5 ЗЕТ

Форма промежуточной аттестации

Экзамен

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

Цели освоения дисциплины

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

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

---

#### Место дисциплины в структуре ОП

---

Дисциплина «Сети и системы передачи информации» Б1.О.09.07 является одной из дисциплин обязательной части учебного плана подготовки 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»; «Информационные технологии».

---

#### Требования к результатам освоения

---

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

- Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности; (ОПК-2)
- Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности; (ОПК-9)

---

#### Содержание дисциплины

---

##### Раздел 1. Основные принципы построения современных инфокоммуникационных сетей. Эволюция технологий.

Тенденции развития инфокоммуникаций. Услуги в инфокоммуникациях. Классификация сетевых технологий. Модели ISO/OSI, TCP/IP, NGN. Организации, стандартизирующие решения в области телекоммуникаций. Особенности построения и развития сетей связи в РФ

##### Раздел 2. Технология TCP/IP: протокол IP.

0IP версий 4 и 6. Адресация, распределение адресного пространства, распределение адресов, DNS, структура заголовков, алгоритм обработки пакета на узле.

##### Раздел 3. Маршрутизация в IPсетях.

Понятие маршрутизации. Внешняя и внутренняя маршрутизация. Формирование таблиц маршрутизации. Понятие автономной системы. Типы маршрутизаторов. Принципы

построения маршрутизаторов. Алгоритм Белмана-Форда. Алгоритм Дейстры. Понятие метрики. Основные протоколы маршрутизации: RIP, OSPF, IS-IS, BGP.

#### Раздел 4. Технологии уровня доступа.

Эволюция Ethernet: от 10 Мбит/с к 10 Гбит/с. Особенности формирования кадра Ethernet: уровни LLC и MAC. Метод доступа CSMA/CD. Формат кадра Ethernet. Протокол ARP. Коммутаторы Ethernet: неуправляемые и управляемые. Требования к неблокирующему режиму работы коммутатора. Способы организации неблокирующего коммутатора. СКС для Ethernet: виды кабеля, разъемов, обжимка. Использование сетей PON для организации доступа абонентов. Использование существующей телефонной линии: xDSL, протокол PPP.

#### Раздел 5. Технологии транспортных сетей.

Рабочая среда E1. Формирование PDH. Технология SDH – формирование нагрузки, использование для организации магистрали. Понятие синхронизации. Технология ATM для построения транспортных сетей. Технология DWDM, принципы волнового мультиплексирования. Технология MPLS.

#### Раздел 6. Методы управления сетью.

Функции транспортного уровня, управление трафиком на транспортном уровне. Протокол UDP. Протокол TCP. Установление соединения. Квитирование. Медленный старт. Алгоритм RED и его влияние на работу TCP. Версии TCP. Влияние протоколов транспортного уровня на работу приложений. Управление сетевыми элементами. Протокол SNMP. Маршрутизация как способ управления сетью.

#### Раздел 7. Беспроводные сети связи.

Классификация беспроводных сетей. Беспроводные технологии доступа. Сотовые сети, особенности построения. Процедура идентификации абонента. Принципы организации беспроводных каналов на магистральных участках и в труднодоступных районах.

#### Раздел 8. Услуги в NGN и качество обслуживания.

Классификация услуг в NGN. Требования к услугам: показатели качества обслуживания, стандарты и рекомендации. Качество обслуживания и качество восприятия. Источники ухудшения качества услуги. IPтелефония и IPTV как примеры мультисервисных услуг: проблемы и их решения.

#### Раздел 9. Обработка и хранение информации в глобальных сетях.

Управление информационными потоками в глобальных сетях, хранение информации, в т.ч. распределенное. Архитектура центров обработки данных. Распределенные облачные вычисления

---

Общая трудоемкость дисциплины

180 час(ов), 5 ЗЕТ

Форма промежуточной аттестации

Экзамен. Курсовой проект

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

---

Цели освоения дисциплины

Целью преподавания дисциплины «Основы информационной безопасности»

является:

изучение вопросов управления информационной безопасностью

---

Место дисциплины в структуре ОП

---

Дисциплина «Основы информационной безопасности» Б1.О.10.01 является дисциплиной обязательной части учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Изучение дисциплины «Основы информационной безопасности» основывается на базе знаний, умений и компетенций, полученных студентами в ходе освоения школьных курсов.

---

Требования к результатам освоения

---

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

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

---

Содержание дисциплины

---

#### Раздел 1. Оценка рисков информационной безопасности

Основные составляющие информационной безопасности. Угрозы информационной безопасности в информационных системах. Основные определения и критерии, угрозы целостности и конфиденциальности.

#### Раздел 2. Стандарты управления информационной безопасностью

Государственные стандарты в области ИБ РФ. Оценочные стандарты в информационной безопасности. Оранжевая книга. Международный стандарт ISO/IEC 15408. Критерии оценки безопасности информационных систем. Стандарты управления информационной безопасностью BS 7799 и ISO/IEC 17799. Их основные положения. Международный стандарт ISO/IEC 27001:2005 "Системы управления информационной безопасностью. Требования"

#### Раздел 3. Принципы построения интегрированных систем информационной безопасности

Создание политик ИБ предприятия. Принципы обеспечения безопасности инфраструктуры. Принципы обеспечения безопасности периметра сети телекоммуникационной системы. Регулирование правил работы СКУД. Регулирование правил удаленного доступа средствами VPN. Контроль безопасности конечных устройств. Контроль безопасности IP-телефонии.

#### Раздел 4. Принципы организации аудита систем информационной безопасности

Основные техники проведения аудита систем ИБ. Разработка методики проведения аудита систем ИБ. Основные средства проведения аудита систем ИБ.

#### Раздел 5. Аудит инфраструктуры ИБ, интегрированных сервисов телефонии и беспроводного доступа

Основные механизмы и принципы проведения аудита ИБ инфраструктуры предприятия.

Основные механизмы и принципы проведения аудита ИБ систем IP-телефонии, а также систем беспроводного доступа Wi-Fi

#### Раздел 6. Аудит систем удаленного и локального доступа

Основные механизмы и принципы проведения аудита ИБ СКУД предприятия, а также систем удаленного доступа с использованием технологий виртуальных частных сетей

#### Раздел 7. Введение в оценку и аудит ИБ путем выявления угроз ИБ «на лету»

Введение в «этический хакинг». Основные принципы его организации. Составление плана проведения тестирования целевой системы (инфраструктуры). Отношение к законодательству и регуляторам. Составление отчета и рекомендаций на основе проведенного тестирования.

#### Раздел 8. Проведение комплекса процедур цифрового расследования в информационных и компьютерных системах

DigitalForensic. Расследование инцидентов. Утилиты для расследования инцидентов. Информация об истории посещения сайтов, кукисах, букмарках, скачанных файлах, заполненных формах, сохраненных логинах и т.д.

#### Раздел 9. Основные принципы построения SIEM

Средства визуализации элементов ИБ. Визуализация статистики по инцидентам ИБ. Комплексные системы мониторинга ИБ. Средства сбора отчетов и Logов. Основные принципы работы SIEM систем. Составление отчетов по ИБ.

#### Раздел 10. Управление информационной безопасностью на государственном уровне.

##### Общие принципы и российская практика

Организационно-правовые формы управления безопасностью. Предпосылки развития государственного управления в сфере информационной безопасности. Общая методология и структура организационного обеспечения информационной безопасности на уровне государств. Общая политика России в сфере информационной безопасности. Структура органов государственной власти, обеспечивающих информационную безопасность в РФ.

---

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет. Курсовая работа

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

---

Цели освоения дисциплины

Целью преподавания дисциплины «Организационное и правовое обеспечение информационной безопасности» является:

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.О.10.02 является дисциплиной обязательной части 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:

- Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности; (ОПК-5)
  - Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю; (ОПК-6)
  - Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности; (ОПК-8)
  - Способен воспринимать межкультурное разнообразие общества в социально-историческом, этическом и философском контекстах (УК-5)
- 

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

---

Цели освоения дисциплины

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

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

---

Место дисциплины в структуре ОП

---

Дисциплина «Методы и средства криптографической защиты информации» Б1.О.10.03 является одной из дисциплин обязательной

части учебного плана подготовки 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 «Основы информационной безопасности».

---

#### Требования к результатам освоения

---

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

- Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности; (ОПК-9)
- Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений; (ОПК-12)

---

#### Содержание дисциплины

---

##### Раздел 1. Основные понятия

Криптография. Цели криптографии. История развития криптографии. Классификация криптографических методов. Обеспечение конфиденциальности, целостности, неотказуемости, аутентичности, неотслеживаемости информации. Основные понятия: шифр, открытый текст, шифртекст, электронная подпись, хэш-функция,

##### Раздел 2. Основные характеристики шифров

Алгебраическая модель шифра. Алгебраическая модель шифра замены. Алгебраическая модель шифра перестановки. Алгебраическая модель шифра гаммирования

##### Раздел 3. Симметричная криптография. Электронная подпись

Классификация симметричных криптографических систем. Требования к блочным шифрам. Требования к поточным шифрам. Криптографические параметры узлов и блоков блочных шифров. Базовые криптографические преобразования блочных шифров. Способы реализации блочных шифров. Процедура развертывания ключа.

---

#### Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

#### Форма промежуточной аттестации

Зачет

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

##### Цели освоения дисциплины

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

Целью преподавания дисциплины является изучение вопросов основ защиты информации в телекоммуникационных системах. Дисциплина «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.О.10.04 является одной из дисциплин обязательной 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 «Основы информационной безопасности».

##### Требования к результатам освоения

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

- Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности; (ОПК-9)
- Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений; (ОПК-12)

##### 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 квитируванием, память типа FIFO

### Раздел 3. Установка и настройка Arduino в ОС Windows

Установка Arduino IDE, Запуск Arduino IDE, Подключение Arduino к компьютеру, Настройка Arduino IDE на работу с ArduinoUno, загрузка скетчей, Среда разработки AtmelStudio

### Раздел 4. Классификация типов программно-аппаратных средств защиты информации

Идентификация и аутентификация, управление доступом, протоколирование и аудит, криптография, экранирование.

### Раздел 5. Методы построения программно-аппаратных средств защиты информации

Обзор методов построения: 1. Средств, разработанных для защиты информации от НСД в информационных сетях, но допускающие применение и в персональных компьютерах; 2. Средств, принципиально применимых только в компьютерных сетях и предназначенные для разделения информационных потоков, — так называемые межсетевые экраны; 3. Средств, принципиально предназначенных для защиты информации от НСД в персональных компьютерах.

---

Общая трудоемкость дисциплины

180 час(ов), 5 ЗЕТ

Форма промежуточной аттестации

Экзамен

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

---

Цели освоения дисциплины

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

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

---

Место дисциплины в структуре ОП

---

Дисциплина «Защита информации от утечки по техническим каналам» Б1.О.10.05 является одной из дисциплин обязательной части учебного плана подготовки 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 в операционных системах».

---

## Требования к результатам освоения

---

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

- Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности; (ОПК-9)
  - Способен проводить работы по установке, настройке и испытаниям защищенных технических средств обработки информации (ПК-12)
  - Способен проводить контроль эффективности защиты информации от утечки за счет побочных электромагнитных излучений и наводок (ПК-13)
- 

## Содержание дисциплины

---

### Раздел 1. Введение

Предмет, цели, задачи и содержание курса инженернотехнической защиты информации (ИТЗИ). Роль и место курса в подготовке специалистов по организации защиты информации в государственных и коммерческих структурах. Базовые знания, необходимые для изучения курса. Рекомендуемые учебные пособия

### Раздел 2. Объекты информационной защиты

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

### Раздел 3. Технические средства охраны объектов инфокоммуникаций

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

### Раздел 4. Способы и средства добывания информации техническими средствами.

#### Технические каналы утечки информации

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

вещественные каналы утечки информации. Комплексирование технических каналов утечки информации.

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

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

Общая трудоемкость дисциплины

144 час(ов), 4 ЗЕТ

Форма промежуточной аттестации

Экзамен

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

Цели освоения дисциплины

Целью преподавания дисциплины «Гуманитарные аспекты информационной безопасности» является:

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

Место дисциплины в структуре ОП

Дисциплина «Гуманитарные аспекты информационной безопасности» Б1.О.10.06 является одной из дисциплин обязательной части учебного плана подготовки 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 «Основы информационной безопасности».

---

## Требования к результатам освоения

---

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

- Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства; (ОПК-1)
  - Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни (УК-6)
  - Способен формировать нетерпимое отношение к коррупционному поведению (УК-10)
- 

## Содержание дисциплины

---

### Раздел 1. Место и роль проблем информационной безопасности в становлении современного информационного общества

Нормативные документы в области информационной безопасности. Структура и задачи органов, обеспечивающих ИБ. Гуманитарная сущность ИБ.

### Раздел 2. Проблемы обеспечения баланса интересов личности, общества и государства в информационной сфере

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

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

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

### Раздел 4. Основы компьютерной этики

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

### Раздел 5. Компьютерные правонарушения

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

### Раздел 6. Интеллектуальная собственность

Понятие интеллектуальной собственности. Виды интеллектуального права: авторское право, смежные права, патентное право, права на средства индивидуализации, право на секреты производства. Нарушение прав интеллектуальной собственности.

### Раздел 7. Неприкосновенность частной жизни

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

### Раздел 8. Риски использования информационных технологий

Понятие рисков в сфере информационных технологий. Риски, вызванные утечкой информации и использованием ее конкурентами или сотрудниками в целях, которые могут навредить. Риски технических сбоев работы аппаратного и программного



обеспечения, каналов передачи информации. Процессы минимизации ИТ-рисков

---

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

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

Цели освоения дисциплины

---

Целью преподавания дисциплины «Основы управления проектами» является:

Цель преподавания дисциплины - познакомить студентов с современными концепциями управления проектами, показать связь между управлением проектами и финансовым менеджментом, маркетингом, управлением персоналом и стратегиями развития компании. Познакомить с технологиями и инструментарием в сфере управления проектами. Дисциплина «Основы управления проектами» должна обеспечивать формирование фундамента подготовки бакалавров, а также создавать необходимую базу для успешного овладения последующими специальными дисциплинами учебного плана. Она должна способствовать развитию творческих способностей студентов, умению формулировать и решать задачи изучаемой специальности, умению творчески применять и самостоятельно повышать свои знания.

---

Место дисциплины в структуре ОП

---

Дисциплина «Основы управления проектами» Б1.О.10.07 является одной из дисциплин обязательной части учебного плана подготовки 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 «Экономика».

---

Требования к результатам освоения

---

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

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

- Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений; (ОПК-12)
- Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений (УК-2)
- Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде (УК-3)
- Способен принимать обоснованные экономические решения в различных областях жизнедеятельности (УК-9)

---

#### Содержание дисциплины

---

##### Раздел 1. Теоретические основы проектной деятельности

Определение проекта. Его основные характеристики и измерения. Элементы проектной деятельности. Классификация проектов. Содержание и процессы управления проектами

##### Раздел 2. Технология проектной деятельности: жизненный цикл проекта, его основные этапы

Методология и методика предпроектного анализа (анализ ситуации). Управление интеграцией (содержанием) проекта. Мобилизация ресурсов проекта.

##### Раздел 3. Разработка и управление ресурсными подсистемами проекта

Управление временем проекта. Управление стоимостью проекта. Управление качеством проекта. Управление командой проекта. Управление коммуникациями проекта.

Управление рисками проекта

##### Раздел 4. Мониторинг реализации проекта

Мониторинг и контроль работ проекта. Мониторинг коммуникаций. Мониторинг рисков.

##### Раздел 5. Управление изменениями

План и контроль изменений. Интегрированный контроль изменений

##### Раздел 6. Оценка эффективности реализации проекта и завершение проекта

Оценка и управление стоимостью проекта. Оценка и управление качеством. Ключевые показатели эффективности проекта. Закрытие проекта.

---

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

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

Цели освоения дисциплины

Целью преподавания дисциплины «Основы управления информационной безопасностью» является:

изучение вопросов управления информационной безопасностью. Должна обеспечивать формирование фундамента подготовки будущих специалистов в

области формирования моделей угроз, оценки рисков информационных инфокоммуникационных систем, формирование адекватных методов и средств обеспечения информационной безопасности, а также, создавать необходимую базу для успешного овладения последующими специальными дисциплинами учебного плана. Она должна способствовать развитию творческих способностей студентов, умению формулировать и решать задачи изучаемой специальности, умению творчески применять и самостоятельно повышать свои знания.

---

Место дисциплины в структуре ОП

---

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

---

Требования к результатам освоения

---

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

- Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности; (ОПК-5)
- Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю; (ОПК-6)
- Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты; (ОПК-10)

---

Содержание дисциплины

---

#### Раздел 1. Оценка рисков информационной безопасности

Основные составляющие информационной безопасности. Угрозы информационной безопасности в информационных системах. Основные определения и критерии, угрозы целостности и конфиденциальности.

#### Раздел 2. Стандарты управления информационной безопасностью

Государственные стандарты в области ИБ РФ. Оценочные стандарты в информационной безопасности. Оранжевая книга. Международный стандарт ISO/IEC 15408. Критерии оценки безопасности информационных систем. Стандарты управления информационной

безопасностью BS 7799 и ISO/IEC 17799. Их основные положения Международный стандарт ISO/IEC 27001:2005 "Системы управления информационной безопасности. Требования"

### Раздел 3. Принципы построения интегрированных систем информационной безопасности

Создание политик ИБ предприятия. Принципы обеспечения безопасности инфраструктуры. Принципы обеспечения безопасности периметра сети телекоммуникационной системы. Регулирование правил работы СКУД. Регулирование правил удаленного доступа средствами VPN. Контроль безопасности конечных устройств. Контроль безопасности IP-телефонии.

### Раздел 4. Принципы организации аудита систем информационной безопасности

Основные техники проведения аудита систем ИБ. Разработка методики проведения аудита систем ИБ. Основные средства проведения аудита систем ИБ.

### Раздел 5. Аудит инфраструктуры ИБ, интегрированных сервисов телефонии и беспроводного доступа

Основные механизмы и принципы проведения аудита ИБ инфраструктуры предприятия. Основные механизмы и принципы проведения аудита ИБ систем IP-телефонии, а также систем беспроводного доступа Wi-Fi

### Раздел 6. Аудит систем удаленного и локального доступа

Основные механизмы и принципы проведения аудита ИБ СКУД предприятия, а также систем удаленного доступа с использованием технологий виртуальных частных сетей

### Раздел 7. Введение в оценку и аудит ИБ путем выявления угроз ИБ «на лету»

Введение в «этический хакинг». Основные принципы его организации. Составление плана проведения тестирования целевой системы (инфраструктуры). Отношение к законодательству и регуляторам. Составление отчета и рекомендаций на основе проведенного тестирования.

### Раздел 8. Проведение комплекса процедур цифрового расследования в информационных и компьютерных системах

DigitalForensic. Расследование инцидентов. Утилиты для расследования инцидентов. Информация об истории посещения сайтов, кукисах, букмарках, скачанных файлах, заполненных формах, сохраненных логинах и т.д.

### Раздел 9. Основные принципы построения SIEM

Средства визуализации элементов ИБ. Визуализация статистики по инцидентам ИБ. Комплексные системы мониторинга ИБ. Средства сбора отчетов и Logов. Основные принципы работы SIEM систем. Составление отчетов по ИБ.

### Раздел 10. Управление информационной безопасностью на государственном уровне.

#### Общие принципы и российская практика

Организационно-правовые формы управления безопасностью. Предпосылки развития государственного управления в сфере информационной безопасности. Общая методология и структура организационного обеспечения информационной безопасности на уровне государств. Общая политика России в сфере информационной безопасности. Структура органов государственной власти, обеспечивающих информационную безопасность в РФ.

---

Общая трудоемкость дисциплины

180 час(ов), 5 ЗЕТ

Форма промежуточной аттестации

Экзамен

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

Цели освоения дисциплины

Целью преподавания дисциплины «Комплексная защита объектов информатизации» является:

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

Место дисциплины в структуре ОП

Дисциплина «Комплексная защита объектов информатизации» Б1.О.10.09 является одной из дисциплин обязательной части учебного плана подготовки 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 в операционных системах».

Требования к результатам освоения

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

- Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю; (ОПК-6)
- Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты; (ОПК-10)
- Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений; (ОПК-12)

Содержание дисциплины

### Раздел 1. Введение в информационно -аналитическую деятельность комплексной безопасности (ИАДКБ)

Цели, задачи, объект, предмет информационно-аналитической деятельности комплексной безопасности (далее – ИАДКБКБ). Специфика ИАДКБ. Терминология. Особенности развития ИАДКБ в России. Основные принципы аналитической деятельности. Понятие информационно- аналитических технологий.

### Раздел 2. Первичная обработка информации.

Анализ модельной информации. Определение основных категорий и понятий. Выработка

рабочей гипотезы. Конкретизация цели и задач исследования.

Раздел 3. Методика информационного поиска.

Поиск, отбор, экспресс-анализ первичных данных. Оптимизация поиска ресурсов удаленного доступа. Оптимизация поиска ресурсов удаленного доступа

Раздел 4. Анализ информативности источников.

Проблема активной фильтрации сообщений. Качественные характеристики информации. Режимы восприятия информации. Атрибуция сообщений

Раздел 5. Оценка полноты, непротиворечивости и достоверности информации. Технология создания аналитических документов

Критерии, параметры ограничения логической непротиворечивости и достоверности информации.

Раздел 6. Отчетные документы ИАДКБ.

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

---

Общая трудоемкость дисциплины

180 час(ов), 5 ЗЕТ

Форма промежуточной аттестации

Экзамен

### ***Б1.О.11.01 Основы радиотехники***

---

Цели освоения дисциплины

---

Целью преподавания дисциплины «Основы радиотехники» является: изучение основ радиотехнических систем передачи информации и подготовка студентов к использованию полученных знаний в решении конкретных практических задач по эксплуатации этих систем и входящих в их состав устройств

---

Место дисциплины в структуре ОП

---

Дисциплина «Основы радиотехники» Б1.О.11.01 является дисциплиной обязательной части учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Изучение дисциплины «Основы радиотехники» основывается на базе знаний, умений и компетенций, полученных студентами в ходе освоения школьных курсов.

---

Требования к результатам освоения

---

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

- Способен проводить работы по установке, настройке, испытаниям и техническому обслуживанию средств защиты информации от утечки по техническим каналам; (ОПК-3,1)
- Способен проводить работы по установке, настройке, испытаниям и техническому обслуживанию средств защиты информации от несанкционированного доступа; (ОПК-3,2)
- Способен проводить контроль эффективности защиты информации от утечки по техническим каналам; (ОПК-3,3)
- Способен проводить контроль защищенности информации от несанкционированного доступа; (ОПК-3,4)

---

## Содержание дисциплины

---

### Раздел 1. Введение. Источники и векторы электромагнитного поля

Место и назначение дисциплины. Векторы электромагнитного поля. Свободные и связанные заряды. Токи проводимости и переноса. Плотности заряда и тока.

Электромагнитные параметры среды. Классификация сред.

### Раздел 2. Уравнения Максвелла. Граничные условия. Энергетический баланс ЭМП.

Уравнения Максвелла в интегральной и дифференциальной формах. Закон сохранения заряда и уравнение непрерывности. Сторонние источники. Монохроматическое ЭМП. Комплексная диэлектрическая проницаемость среды. Граничные условия для касательных и нормальных составляющих векторов электромагнитного поля для общего случая и на идеально проводящей поверхности. Энергетический баланс ЭМП. Теорема Умова-Пойнтинга.

### Раздел 3. Методы решения уравнений Максвелла

Однородная и неоднородная система уравнений Максвелла. Однородное и неоднородное волновое уравнение. Единственность решения. Скалярный и векторный потенциал. Внутренняя и внешняя задача. Функция Грина.

### Раздел 4. Направляющие системы и направляемые волны.

Типы направляющих систем и направляемых волн. Волны классов Т, Е и Н. Структура и свойства ЭМП в волноводах. Критическая частота. Режимы полей в волноводах. Фазовая и групповая скорости. Прямоугольные волноводы. Решение волновых уравнений для продольных составляющих полей классов Е и Н. Передаваемая мощность и затухание основной волны. Элементы возбуждения, выбор размеров поперечного сечения, структура полей высших типов. Круглый волновод, структура полей, применение ряда волн в технике связи. Коаксиальный волновод, структура поля волны класса Т, условие одноволнового режима, волновое сопротивление, использование в технике связи. Полосковые линии, структура поля, выбор поперечных размеров. Микрополосковые линии. Линии передачи оптического диапазона – световоды. Затухание волн в световодах. Дисперсионные искажения.

### Раздел 5. Классификация радиоэлектронных средств (РЭС) и радиотехнических систем (РТС)

Классификация РЭС по степени сложности. Классификация РТС по назначению. Основные свойства сообщений и сигналов различных видов связи. Классификация РТС передачи информации по способу представления непрерывных и дискретных сообщений в системе. Классификация систем передачи информации по типу среды распространения электромагнитных волн. Диапазоны электромагнитных волн, применяемых в радиотехнике, и особенности их распространения в различных средах

### Раздел 6. Системные параметры РТС передачи информации

Обобщенная структурная схема одноканальной РТС передачи информации. Основные операции над сигналами в передающей части РТС (способ передачи). Основные операции над сигналами в приемной части РТС (способ приема). Общие свойства радиоканалов связи. Надежность, эффективность, аппаратная надежность, помехоустойчивость, пропускная способность, экономичность РТС передачи информации. Основные критерии для оценки помехоустойчивости: вероятностный, энергетический

#### Раздел 7. Излучение радиоволн. Элементарные излучатели

Излучение радиоволн. Элементарный электрический излучатель. Понятие ближней и дальней зоны излучения. Элементарный магнитный излучатель.

#### Раздел 8. Особенности распространения радиоволн

Особенности распространения ультракоротких волн. Многолучевое распространение, интерференция лучей, общие и селективные замирания. Разнесенный прием радиосигналов и его разновидности: разнесение в пространстве, по частоте, по времени, по поляризации. Способы использования образцов сигнала при разнесенном приеме. Мультипликативные помехи и их описание законом Релея. Расчет вероятности перерыва связи при разнесенном приеме. Передача двоичных сигналов по радиоканалам с помощью амплитудной, частотной и фазовой модуляции и демодуляции.

#### Раздел 9. Распространение радиоволн в средах

Распространение и отражение радиоволн в помещениях. Понятие диффузного рассеивания и зеркального отражения радиоволн. Оценка дальности связи

#### Раздел 10. Основные характеристики антенн и их типы

Основные характеристики антенн. Электрически малые антенны, их типы и применение. Микрорешетчатые антенны. IFA, IFA, PIFA.

---

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

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

---

Цели освоения дисциплины

Целью преподавания дисциплины «Защита в операционных системах» является:

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



---

## Место дисциплины в структуре ОП

---

Дисциплина «Защита в операционных системах» Б1.О.11.02 является дисциплиной обязательной части учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Изучение дисциплины «Защита в операционных системах» основывается на базе знаний, умений и компетенций, полученных студентами в ходе освоения школьных курсов.

---

## Требования к результатам освоения

---

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

- Способен проводить работы по установке, настройке, испытаниям и техническому обслуживанию средств защиты информации от утечки по техническим каналам; (ОПК-3,1)
  - Способен проводить работы по установке, настройке, испытаниям и техническому обслуживанию средств защиты информации от несанкционированного доступа; (ОПК-3,2)
  - Способен проводить контроль эффективности защиты информации от утечки по техническим каналам; (ОПК-3,3)
  - Способен проводить контроль защищенности информации от несанкционированного доступа; (ОПК-3,4)
- 

## Содержание дисциплины

---

### Раздел 1. История развития операционных систем.

История разработки ОС MSDOS, Windows и Unix. Версии ОС. Установка и модернизация Windows Server. Введение в Server Core.

### Раздел 2. Система управления доступом в ОС MS Windows.

Основные компоненты ОС MS Windows. Модель операционной системы. Различие между клиентской и серверной версии. Системные процессы, драйвера, ядро. Вводится понятие реестр операционной системы. Управление сервисами и процессами. Система журналирования

### Раздел 3. Роли ОС MS Windows Server. Реализация доменных служб ActiveDirectory.

Развертывание на основе ролей. Развертывание серверов с конкретными ролями. Знакомство с доменными службами ActiveDirectory, реализация доменных служб AD, управление пользователями, группами, компьютерами, внедрение групповой политики. Понятие леса, домена.

### Раздел 4. Роли ОС MS Windows Server. Реализация доменных служб ActiveDirectory.

Контроль учетных записей, разрешения для файлов и папок, блокировка учетной записи и политики паролей, детальные политики паролей, возможности аудита, функции шифрования данных. Обеспечение безопасности файлов и папок. Аудит файлов. Шифрование файлов. Групповая политика.

### Раздел 5. Хранилище Windows Server.

Многоуровневые пространства хранения. Создание пространств хранения. Ограничения

пулов хранения. Создание виртуального диска. Работа с iSCSI хранилищами. Общие папки NFS и CIFS.

Раздел 6. Реализация системы безопасности сети в ОС MS Windows.

Утилиты по настройке сети. Угрозы сетевой безопасности, реализация брандмауэров. Настройка брандмауэра Windows. Защита доступа к сети.

Раздел 7. Дополнительные возможности Active Directory.

Сайты в ActiveDirectory. Миграция, слияние и модификация ActiveDirectory. Центр сертификации.

Раздел 8. Внедрение программ обеспечения безопасности в ОС MS Windows.

Установка дополнительной системы защиты информации, для упрощения управлением доступом к файлам, на примере системы SearchInform.

---

Общая трудоемкость дисциплины

180 час(ов), 5 ЗЕТ

Форма промежуточной аттестации

Экзамен

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

---

Цели освоения дисциплины

Целью преподавания дисциплины «Криптографические протоколы» является: изучение вопросов основ криптографической защиты информации в телекоммуникационных системах. 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.О.11.03 является одной из дисциплин обязательной 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:

- Способен проводить работы по установке, настройке, испытаниям и техническому обслуживанию средств защиты информации от утечки по техническим каналам; (ОПК-3,1)
- Способен проводить работы по установке, настройке, испытаниям и техническому обслуживанию средств защиты информации от несанкционированного доступа; (ОПК-3,2)
- Способен проводить контроль эффективности защиты информации от утечки по техническим каналам; (ОПК-3,3)
- Способен проводить контроль защищенности информации от несанкционированного доступа; (ОПК-3,4)

---

## 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. Принципы построения систем шифрования

Введение в криптографию. Типы криптосистем. Модель системы шифрования. Способы шифрования. Влияние ошибок в криптограмме на дешифрование.

### Раздел 3. 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 4. 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 5. 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 блочных шифров. Стандарты шифрования AES, ГОСТ 3 34.12-15.

### Раздел 6. 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 блочных шифров. Стандарты шифрования AES, ГОСТ 3 34.12-15.

### Раздел 7. Поточковые шифры

Принципы построения поточковых шифров. Линейный рекуррентный регистр и его свойства. Нелинейные узлы усложнения, используемые для построения поточковых шифров. Нерегулярное тактирование в поточковых шифрах. Основные методы криптоанализа поточковых шифров. Анализ шифра A5 стандарта GSM.

### Раздел 8. Поточковые шифры

Принципы построения поточковых шифров. Линейный рекуррентный регистр и его свойства. Нелинейные узлы усложнения, используемые для построения поточковых шифров. Нерегулярное тактирование в поточковых шифрах. Основные методы криптоанализа поточковых шифров. Анализ шифра A5 стандарта GSM.

#### Раздел 9. 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 10. 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 11. 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.

#### Раздел 12. Управление ключами в симметричных криптосистемах

Модель управления ключами. Этапы жизненного цикла ключа. Распределение ключей на основе ЦРК и доверенных каналов. Распределение ключей в интерактивном режиме с использованием ЦРК.

---

Общая трудоемкость дисциплины

180 час(ов), 5 ЗЕТ

Форма промежуточной аттестации

Экзамен

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

---

Цели освоения дисциплины

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

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

---

Место дисциплины в структуре ОП

---

Дисциплина «Основы построения защищенных компьютерных сетей» Б1.О.11.04 является одной из дисциплин обязательной части учебного плана подготовки 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 в операционных системах»; «Основы информационной безопасности».

---

#### Требования к результатам освоения

---

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

- Способен проводить работы по установке, настройке, испытаниям и техническому обслуживанию средств защиты информации от утечки по техническим каналам; (ОПК-3,1)
- Способен проводить работы по установке, настройке, испытаниям и техническому обслуживанию средств защиты информации от несанкционированного доступа; (ОПК-3,2)
- Способен проводить контроль эффективности защиты информации от утечки по техническим каналам; (ОПК-3,3)
- Способен проводить контроль защищенности информации от несанкционированного доступа; (ОПК-3,4)

---

#### Содержание дисциплины

---

##### Раздел 1. Сетевые атаки

Стадии проведения сетевой атаки. Классификации сетевых угроз, уязвимостей и атак. Атаки на реализации сетевых протоколов, отдельные узлы и службы. Основные механизмы проведения сетевых атак на различных уровнях модели ISO/OSI. Проблемы обеспечения конфиденциальности, целостности и доступности информации на различных уровнях модели ISO/OSI

##### Раздел 2. Механизмы реализации атак в сетях TCP/IP

Удаленное определение версии ОС с использованием особенностей реализации стека протоколов TCP/IP. Методы сканирования портов. Методы обнаружения пакетных сниферов. Методы обхода МЭ

##### Раздел 3. Методы перехвата сетевых соединений в сетях TCP/IP

Импersonация вслепую. Десинхронизация TCP-соединений. Атаки, направленные на сетевую инфраструктуру

##### Раздел 4. Примеры сетевых атак в сетях TCP/IP. Технические меры защиты от сетевых атак

Принуждение к ускоренной передаче. Атаки, направленные на отказ в обслуживании. Изменение конфигурации и состояния хостов. Недостатки протоколов семейства TCP/IP с точки зрения обеспечения безопасности информации. Технические меры защиты от сетевых атак

##### Раздел 5. Криптографические протоколы обеспечения безопасности

Протоколы аутентификации на прикладном уровне. Протокол Kerberos. Протоколы аутентификации на транспортном уровне. Протокол SSL/TLS. Достоинства и недостатки аутентификации на различных уровнях модели ISO/OSI

##### Раздел 6. Защита виртуальных частных сетей (VPN)

Назначение, основные возможности, принципы функционирования и варианты реализации VPN. Организация туннелирования на различных уровнях модели ISO/OSI. Достоинства и недостатки применения VPN. Протокол IPSEC. Протоколы AH и ESP. Особенности работы протокола IPSEC в туннельном и транспортном режимах. Протокол

управления ключами ISAKMP/Oakley. Использование протокола L2TP для организации виртуальных частных сетей

#### Раздел 7. Разработка защищенных сетевых приложений

Аутентификация, шифрование, обеспечение целостности с использованием программного интерфейса SSPI. Программный интерфейс Open SSL

#### Раздел 8. Средства защиты локальных сетей при подключении к Интернет

Межсетевые экраны (МЭ). Место и роль МЭ в обеспечении сетевой безопасности.

Классификация МЭ. Требования к МЭ. Основные возможности и схемы развертывания МЭ. Достоинства и недостатки МЭ. Построение правил фильтрации. Методы сетевой трансляции адресов (NAT). Шлюзы уровня приложений. Реализация сетевой политики безопасности с использованием МЭ. Методы обхода межсетевых экранов

#### Раздел 9. Средства и методы предотвращения и обнаружения вторжений

Системы обнаружения вторжений (СОВ). Назначение и возможности средств обнаружения вторжений на хосты, протоколы и сетевые службы. Место и роль средств обнаружения вторжений в общей системе обеспечения сетевой безопасности.

Классификация СОВ. Выявление атак на основе сигнатур атак и выявления аномалий.

Аудит прикладных служб. Средства обнаружения уязвимостей сетевых служб. Способы противодействия вторжениям. Системы виртуальных ловушек (Honey Pot и Padded Cell)

---

Общая трудоемкость дисциплины

180 час(ов), 5 ЗЕТ

Форма промежуточной аттестации

Экзамен. Курсовая работа

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

---

Цели освоения дисциплины

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

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

---

Место дисциплины в структуре ОП

---

Дисциплина «Основы построения сертифицированных защищенных баз данных РФ» Б1.О.11.05 является одной из дисциплин обязательной части учебного плана подготовки 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 «Основы информационной безопасности».

---

## Требования к результатам освоения

---

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

- Способен проводить работы по установке, настройке, испытаниям и техническому обслуживанию средств защиты информации от утечки по техническим каналам; (ОПК-3,1)
  - Способен проводить работы по установке, настройке, испытаниям и техническому обслуживанию средств защиты информации от несанкционированного доступа; (ОПК-3,2)
  - Способен проводить контроль эффективности защиты информации от утечки по техническим каналам; (ОПК-3,3)
  - Способен проводить контроль защищенности информации от несанкционированного доступа; (ОПК-3,4)
- 

## Содержание дисциплины

---

### Раздел 1. Основные угрозы и средства защиты БД

Причины, виды, основные методы нарушения конфиденциальности в СУБД. Получение несанкционированного доступа к конфиденциальной информации путем логических выводов. SQL-инъекции. Средства обеспечения защиты информации в СУБД.

### Раздел 2. Модели и методы обеспечения безопасности БД

Модели безопасности, применяемые при построении защиты в СУБД. Использование транзакции для изолирования действий пользователей. Блокировки. Ссылочная целостность, триггерная и событийная реализации правил безопасности. Особенности применения криптографических методов. Критерии защищенности БД и АИС.

### Раздел 3. Разработка программ, осуществляющей хранение информации в БД

Основные понятия и классификация систем управления базами данных, общие требования к их разработке. Инфологическое проектирование, обоснование информационных объектов. Составление инфологической организованной модели. Создание таблиц.

### Раздел 4. Работа с файлами БД на низком уровне

Понятие SQL Server. Ознакомление с архитектурой базы данных SQL Graph. SQL Server Компонент Service Broker

---

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

## **Б1.О.11.06 Основы проектирования систем защиты объектов информатизации**

### Цели освоения дисциплины

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

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

### Место дисциплины в структуре ОП

Дисциплина «Основы проектирования систем защиты объектов информатизации» Б1.О.11.06 является одной из дисциплин обязательной 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 «Основы информационной безопасности».

### Требования к результатам освоения

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

- Способен проводить работы по установке, настройке, испытаниям и техническому обслуживанию средств защиты информации от утечки по техническим каналам; (ОПК-3,1)
- Способен проводить работы по установке, настройке, испытаниям и техническому обслуживанию средств защиты информации от несанкционированного доступа; (ОПК-3,2)
- Способен проводить контроль эффективности защиты информации от утечки по техническим каналам; (ОПК-3,3)
- Способен проводить контроль защищенности информации от несанкционированного доступа; (ОПК-3,4)

### Содержание дисциплины

#### Раздел 1. Понятие и сущность информационной безопасности и защиты информации

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

#### Раздел 2. Основные угрозы информационной безопасности

Классификация угроз безопасности по цели реализации угрозы, принципу, характеру и способу её воздействия. Особенности угроз воздействия на объект атаки в зависимости от его состояния и используемых средств атаки. Основные методы и каналы



несанкционированного доступа к информации в информационной системе (ИС). Базовые принципы защиты от несанкционированного доступа к информации в соответствии с нормативно-правовыми документами России. Задачи по защите ИС от реализации угроз.

### Раздел 3. Система защиты информации

Процесс развития средств и методов защиты информации Этапы развития системы защиты информации в настоящее время Комплексный подход к построению системы защиты информации Системный подход к построению системы защиты информации Цели задачи системы защиты информации. Этапы и порядок проведения работ по созданию системы защиты информации. Структура систем защиты информации на современном этапе. Методы (виды) обеспечения защиты информации.

### Раздел 4. Обеспечение режима конфиденциальности при работе с защищаемой информацией

Разрешительная (разграничительная) система доступа должностных лиц, работников к конфиденциальным сведениям, документам и базам данных Допуск должностных лиц, работников к конфиденциальной информации Доступ должностных лиц, работников к конфиденциальным сведениям, документам и базам данных Обязанности должностных лиц, допущенных к сведениям, составляющим коммерческую тайну Порядок предоставления (получения) конфиденциальной информации работникам сторонних организаций, государственным учреждениям

### Раздел 5. Контроль за соблюдением требований информационной безопасности и защиты информации

Основные положения по осуществлению контроля, назначение, цель и задачи контроля. Основные мероприятия по осуществлению контроля. Порядок проведения проверки (контроля) наличия документов и иных носителей информации ограниченного доступа Проведение служебного расследования по фактам утечки конфиденциальной информации, утраты носителей, содержащих такие сведения, а также по фактам грубых нарушений режима конфиденциальности.

---

Общая трудоемкость дисциплины

144 час(ов), 4 ЗЕТ

Форма промежуточной аттестации

Экзамен

## **Б1.О.11.07 Основы построения и функционирования специальных технических средств**

---

Цели освоения дисциплины

Целью преподавания дисциплины «Основы построения и функционирования специальных технических средств» является:

Целью преподавания дисциплины является изучение студентами принципов построения и особенностям функционирования средств инженерно-технической защиты объектов инфокоммуникаций и включает в себя как методы и средства инженерно-технической защиты информации так и технические средства охраны объектов и помещений. В результате изучения дисциплины у студентов должны

сформироваться знания, умения и навыки, позволяющие проводить самостоятельный анализ физических процессов, происходящих в инженернотехнических средствах защиты объектов, как изучаемых в настоящей дисциплине, так и находящихся за ее рамками.

---

Место дисциплины в структуре ОП

---

Дисциплина «Основы построения и функционирования специальных технических средств» Б1.О.11.07 является одной из дисциплин обязательной 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 «Основы информационной безопасности».

---

Требования к результатам освоения

---

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

- Способен проводить работы по установке, настройке, испытаниям и техническому обслуживанию средств защиты информации от утечки по техническим каналам; (ОПК-3,1)
- Способен проводить работы по установке, настройке, испытаниям и техническому обслуживанию средств защиты информации от несанкционированного доступа; (ОПК-3,2)
- Способен проводить контроль эффективности защиты информации от утечки по техническим каналам; (ОПК-3,3)
- Способен проводить контроль защищенности информации от несанкционированного доступа; (ОПК-3,4)

---

Содержание дисциплины

---

#### Раздел 1. Раздел 1. Введение

Предмет, цели, задачи и содержание курса инженернотехнической защиты информации (ИТЗИ). Роль и место курса в подготовке специалистов по организации защиты информации в государственных и коммерческих структурах. Базовые знания, необходимые для изучения курса. Рекомендуемые учебные пособия

#### Раздел 2. 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. Оознавательные 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. Раздел 3. Технические средства охраны объектов инфокоммуникаций

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

Раздел 4. 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. Комплексование технических каналов утечки информации.

Раздел 5. 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

***B1.O.11.08 Метрология, стандартизация и сертификация***

---

Цели освоения дисциплины

Целью преподавания дисциплины «Метрология, стандартизация и сертификация» является:  
обеспечение требований Государственного Образовательного стандарта к

уровню подготовки бакалавров в области метрологии, стандартизации и сертификации. Дисциплина «Метрология, стандартизация и сертификация» должна способствовать расширению общего технического кругозора студентов, развитию их творческих способностей, умению творчески применять и самостоятельно повышать свои знания.

---

#### Место дисциплины в структуре ОП

---

Дисциплина «Метрология, стандартизация и сертификация» Б1.О.11.08 является одной из дисциплин обязательной 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»; «Теория вероятностей и математическая статистика»; «Физика».

---

#### Требования к результатам освоения

---

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

- Способен проводить работы по установке, настройке, испытаниям и техническому обслуживанию средств защиты информации от утечки по техническим каналам; (ОПК-3,1)
- Способен проводить работы по установке, настройке, испытаниям и техническому обслуживанию средств защиты информации от несанкционированного доступа; (ОПК-3,2)
- Способен проводить контроль эффективности защиты информации от утечки по техническим каналам; (ОПК-3,3)
- Способен проводить контроль защищенности информации от несанкционированного доступа; (ОПК-3,4)

---

#### Содержание дисциплины

---

##### Раздел 1. Введение в дисциплину.

Введение в дисциплину. Определение терминов: метрология, техническое регулирование, стандартизация, подтверждение соответствия, сертификация. Значение этих областей знания при разработке, производстве и эксплуатации телекоммуникационного оборудования и средств измерений.

##### Раздел 2. Основы метрологии и теории погрешностей.

Основные термины и определения в области метрологии. Государственная система обеспечения единства измерений. Система единиц величин СИ. Размерности единиц. Виды средств измерений. Эталоны и рабочие средства измерений. Классификация методов и средств измерений. Классификация погрешностей. Систематические погрешности. Случайные погрешности, доверительная вероятность и доверительный интервал. Результат измерения и его погрешность. Погрешности косвенных измерений. Суммирование погрешностей. Нормируемые метрологические характеристики средств измерений. Классы точности средств измерений. Правила представления результатов

измерений. Понятие неопределенности результата измерений.

Раздел 3. Измерительные преобразователи переменного напряжения и тока. Вольтметры и анализаторы спектра.

Измерительные преобразователи переменного напряжения и тока. Вольтметры и анализаторы спектра.

Раздел 4. Аналоговые и цифровые осциллографы.

Наблюдение, измерение и исследование формы электрических сигналов. Классификация осциллографов. Аналоговые осциллографы, типовая структурная схема, метрологические характеристики. Генераторы линейной развертки (непрерывной, ждущей, задержанной). Режим внешней развертки. Осциллографические измерения. Цифровые осциллографы, структурная схема, принципы работы, метрологические характеристики, преимущества по сравнению с аналоговыми осциллографами.

Раздел 5. Цифровые измерения частоты, периода, интервалов времени.

Методы цифровых измерений частотно-временных параметров сигналов: частоты, периода, интервалов времени, отношения частот. Структурные схемы электронно-счетных частотомеров. Опорные генераторы. Источники погрешностей и их нормирование.

Раздел 6. Основные принципы технического регулирования. Отечественная, международная и межгосударственная стандартизация. Подтверждение соответствия и сертификация.

Правовые основы технического регулирования. Основные принципы и теоретическая база стандартизации. Виды стандартов. Отечественная и международная стандартизация в измерениях и технологических процессах. Роль стандартизации в повышении качества, безопасности и конкурентоспособности продукции, в развитии научно-технического и экономического сотрудничества. Сертификация как форма подтверждения соответствия. Правовые основы, системы, схемы и этапы сертификации. Органы по сертификации и их аккредитация. Сертификация средств измерений, средств связи, радиоэлектронных средств.

Раздел 7. Автоматизация измерений. Информационно-измерительные системы. Контроль условий проведения измерений (температура, давление, влажность).

Информационно-измерительные системы. Автоматизация измерений - основные направления. Стандартизованные интерфейсы измерительных систем. Интерфейс МЭК 625 и его модификации (GPIB, HP-IB, IEEE-488). «Виртуальные» средства измерений.

---

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

***Б1.О.11.09 Контроль защищенности ЛВС от несанкционированного доступа (Информационные технологии. Дополнительные главы)***

---

Цели освоения дисциплины

Целью преподавания дисциплины «Контроль защищенности ЛВС от несанкционированного доступа (Информационные технологии. Дополнительные

главы)» является:

Изучение архитектуры, структуры, функции, компонентов беспроводных локальных сетей

---

Место дисциплины в структуре ОП

---

Дисциплина «Контроль защищенности ЛВС от несанкционированного доступа (Информационные технологии. Дополнительные главы)» Б1.О.11.09 является одной из дисциплин обязательной 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 информации от утечки по техническим каналам».

---

Требования к результатам освоения

---

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

- Способен проводить работы по установке, настройке, испытаниям и техническому обслуживанию средств защиты информации от утечки по техническим каналам; (ОПК-3,1)
  - Способен проводить работы по установке, настройке, испытаниям и техническому обслуживанию средств защиты информации от несанкционированного доступа; (ОПК-3,2)
  - Способен проводить контроль эффективности защиты информации от утечки по техническим каналам; (ОПК-3,3)
  - Способен проводить контроль защищенности информации от несанкционированного доступа; (ОПК-3,4)
- 

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

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

### ***Б1.В.01 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.В.01 является дисциплиной части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Изучение дисциплины «Введение в профессию» опирается на знания дисциплин(ы) «Информатика».

Требования к результатам освоения

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

- Способен проводить эксперименты по заданной методике и обработку их результатов; (ОПК-11)
- Способен оценивать угрозы безопасности информации в компьютерных сетях (ПК-6)
- Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач (УК-1)

Содержание дисциплины

Раздел 1. История высшего образования в России и мире. Профессор М.А.Бонч-Бруевич. СПбГУТ. Факультет ИКСС. Кафедра ЗСС

История образования в мире. Первые университеты. Первые университеты в России. Жизнь и основные научные достижения проф. М.А.Бонч-Бруевича. История ЛЭИС – СПбГУТ. Структура факультета ИКСС. История, состав, основные достижения кафедры Защищенных систем связи.

Раздел 2. Структура направления подготовки бакалавров 10.03.01 Информационная безопасность

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

История связи, компьютерные сети, возникновение Internet.

Раздел 6. Хакеры и проблемы информационной безопасности

Феномен хакеров, причины появления, примеры. Актуальность вопросов информационной безопасности в современном мире.

Раздел 7. Информационная война и промышленный шпионаж в современном мире

Информационная война, исторические примеры, примеры из текущих новостей.

Промышленный шпионаж в современном мире – примеры. Актуальность подготовки специалистов в области информационной безопасности.

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

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

Цели освоения дисциплины

Целью преподавания дисциплины «Разработка защищенных сетевых приложений» является:

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

Место дисциплины в структуре ОП



---

Дисциплина «Разработка защищенных сетевых приложений» Б1.В.02 является дисциплиной части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Изучение дисциплины «Разработка защищенных сетевых приложений» опирается на знания дисциплин(ы) «Языки программирования».

---

Требования к результатам освоения

---

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

- Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности; (ОПК-7)
  - Способен анализировать угрозы безопасности информации программного обеспечения (ПК-9)
  - Способен формулировать и обосновывать правила безопасной эксплуатации программного обеспечения (ПК-10)
  - Способен осуществлять мероприятия по противодействию угрозам безопасности информации, возникающим при эксплуатации программного обеспечения (ПК-11)
- 

Содержание дисциплины

---

Раздел 1. Защищенные протоколы

Виртуальные частные сети. Задачи, решаемые VPN. Туннелирование в VPN. Уровни защищенных каналов.

Раздел 2. Интернет-технологии

Архитектура web-сервера. Модель «клиент-сервер». Модель сервера приложений. Трехуровневая архитектура. Взаимодействие компонентов.

Раздел 3. SQL-инъекции

Принцип внедрения SQL-кода в приложения. Особенности языка SQL для реализации инъекций. Уязвимости, используемые при SQL-инъекциях

Раздел 4. Аутентификация на web-сервере

Средства идентификации и аутентификации, методы разделения ресурсов, технологии разграничения доступа.

Раздел 5. Обеспечение доступности web-приложения

Сервис высокой доступности (HA). Кластерная организация web-ресурсов

---

Общая трудоемкость дисциплины

144 час(ов), 4 ЗЕТ

Форма промежуточной аттестации

Экзамен. Курсовая работа

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

#### Цели освоения дисциплины

---

Целью преподавания дисциплины «Основы маршрутизации в компьютерных сетях» является:

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

---

#### Место дисциплины в структуре ОП

---

Дисциплина «Основы маршрутизации в компьютерных сетях» Б1.В.03 является дисциплиной части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Изучение дисциплины «Основы маршрутизации в компьютерных сетях» опирается на знания дисциплин(ы) «Безопасность беспроводных локальных сетей».

---

#### Требования к результатам освоения

---

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

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

#### Содержание дисциплины

---

##### Раздел 1. Введение в коммутируемые сети

Дизайн локальных вычислительных сетей. Конвергированные сети. Сети без границ. Уровни построения сети (ядра, распределения, доступа). Коммутируемые сети. Методы обработки кадров. Понятие коллизий доменов.

##### Раздел 2. Основы коммутации

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. Тэги 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 OSPF для 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. SLAAC и протокол DHCPv6. Настройка SLAAC и DHCPv6. Настройка маршрутизатора в качестве stateless DHCP v6 сервера. Настройка маршрутизатора в качестве stateful клиента. Поиск неисправностей протокола DHCP.

---

Общая трудоемкость дисциплины

144 час(ов), 4 ЗЕТ

Форма промежуточной аттестации

Экзамен

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

Цели освоения дисциплины

---

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

задачи изучаемой специальности, умению творчески применять и самостоятельно повышать свои знания

Место дисциплины в структуре ОП

Дисциплина «Безопасность Astra-Linux» Б1.В.04 является дисциплиной части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Изучение дисциплины «Безопасность Astra-Linux» опирается на знания дисциплин(ы) «Защита в операционных системах».

Требования к результатам освоения

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

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

Содержание дисциплины

#### Раздел 1. История развития ОС Linux

История разработки ОС Unix. Версии ОС. Стандарт POSIX. Развитие проекта GNU, лицензия GNU GPL. Создание и развития дистрибутивов GNU/Linux. Анализ достоинств и недостатков различных операционных систем.

#### Раздел 2. Основы взаимодействия с ОС AstraLinux.

Установка и настройка ОС. Системные компоненты: управления устройствами, файловой системой, пользователями, перезагрузка и отключение. Системные сервисы и команды: сервисы, командный и графический интерфейс. Базовые сетевые службы.

#### Раздел 3. Средства организации единого пространства пользователей.

Единое пространство пользователей (ЕПП) – средства организации пользователей в сети. Механизмы и службы организации ЕПП: механизмы NSS и PAM, службы каталогов LDAP, аутентификация Kerberos, служба AstraLinux Directory, шаблоны конфигурации, сценарии сессии пользователя. Администрирование домена

#### Раздел 4. Управление программными пакетами и резервирование.

Установка и удаление программ. Набор команд dpkg. Комплекса программ apt. Обновление программ и системы. Виды резервного копирования. Планирования резервного копирования. Инфраструктура для управления системой резервного копирования. Утилиты rsync и tar.

#### Раздел 5. Разграничение доступа в ОС AstraLinux.

Идентификация, аутентификация и авторизация. Дискреционное разграничение доступа: определения, Linux-привилегии, средства управления дирекционными правами доступа файлов и СУБД. Мандатное разграничение доступа: определения, привилегии, сетевое взаимодействие, средства управления мандатным доступом, средства управления привилегиями пользователей и процессов. Мандатное разграничение доступом в СУБД и комплексах программ

Раздел 6. Дополнительные механизмы обеспечения безопасности.

Очистка памяти. Изоляция модулей. Маркировка печатных документов. Защита ввода-вывода информации на внешний носитель. Сопоставление пользователя и устройство. Контроль целостности. Режимы киоска и запрета установки исполняемого бита.

Раздел 7. Аудит системы безопасности и восстановление.

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

---

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

### ***Б1.В.05 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.05 является дисциплиной части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Изучение дисциплины «Принципы организации глобальных вычислительных сетей» опирается на знания дисциплин(ы) «Безопасность беспроводных локальных сетей».

---

Требования к результатам освоения

---

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

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

---

Содержание дисциплины

---

### Раздел 1. Иерархический сетевой дизайн

Иерархический дизайн сетей. Архитектура CiscoEnterprise. Модуль сети кампуса, границы сети. Архитектура сетей без границ, средств совместной работы, дата-центров 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 туннелей.

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.06 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.08 является дисциплиной части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Изучение дисциплины «Основы проектирования защищенных инфокоммуникационных систем» опирается на знания дисциплин(ы) «Безопасность беспроводных локальных сетей».

---

Требования к результатам освоения

---

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

- Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений; (ОПК-12)
  - Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни (УК-6)
- 

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.07 Защита речевой информации в помещениях***

---

Цели освоения дисциплины

Целью преподавания дисциплины «Защита речевой информации в помещениях» является:

Обеспечение защищенности выделенных помещений от утечки речевой информации по акустическим и виброакустическим каналам является необходимой задачей реализации мероприятий по регламентированной защите объектов.

---

Место дисциплины в структуре ОП

---

Дисциплина «Защита речевой информации в помещениях» Б1.В.07 является дисциплиной части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Изучение дисциплины «Защита речевой информации в помещениях» опирается на знания дисциплин(ы) «Основы информационной безопасности».

---

Требования к результатам освоения



---

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

- Способен проводить работы по установке, настройке, испытаниям и техническому обслуживанию средств защиты информации от утечки по техническим каналам; (ОПК-3.1)
  - Способен проводить контроль эффективности защиты информации от утечки по техническим каналам; (ОПК-3.3)
  - Способен проводить контроль эффективности защиты акустической (речевой) информации от утечки по техническим каналам (ПК-14)
- 

Содержание дисциплины

---

Раздел 1. 1. Технические каналы утечки информации

Системный подход к защите информации. Характеристика инженерно-технической защиты информации как области информационной безопасности. Основные проблемы инженерно-технической защиты информации. Представление сил и средств защиты информации в виде системы.

Раздел 2. 2. Способы и средства защиты информации от утечки по техническим каналам

Основные концептуальные положения технической защиты информации. Цели и задачи защиты информации. Ресурсы, выделяемые на защиту информации. Принципы защиты информации техническими средствами. Основные направления инженерно-технической защиты информации.

Раздел 3. 3. Методы и средства контроля эффективности технической защиты информации

Контроль эффективности инженерно-технической защиты информации. Виды контроля эффективности инженерно-технической защиты информации. Виды зон контроля. Требования по защите информации от утечки по техническим каналам. Виды технического контроля

Раздел 4. 4. Организация технической защиты информации

Государственная система защиты информации. Основные задачи, структура и характеристика государственной системы противодействия технической защите. Основные руководящие, нормативные и методические документы по защите информации и противодействия технической разведке. Основные организационные и технические меры по защите информации.

---

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

## **Б1.В.08 Защита от перехвата информации в направляющих линиях связи**

### Цели освоения дисциплины

---

Целью преподавания дисциплины «Защита от перехвата информации в направляющих линиях связи» является:

подготовка студентов к профессиональной деятельности в области разработки и применения методов и технических средств защиты линейных сооружений связи от неблагоприятных внешних воздействий и несанкционированного доступа.

---

### Место дисциплины в структуре ОП

---

Дисциплина «Защита от перехвата информации в направляющих линиях связи» Б1.В.08 является дисциплиной части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Изучение дисциплины «Защита от перехвата информации в направляющих линиях связи» опирается на знании дисциплин(ы) «Физика».

---

### Требования к результатам освоения

---

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

- Способен проводить работы по установке, настройке, испытаниям и техническому обслуживанию средств защиты информации от несанкционированного доступа; (ОПК-3,2)
  - Способен проводить контроль защищенности информации от несанкционированного доступа; (ОПК-3,4)
  - Способен проводить контроль эффективности защиты информации от утечки за счет побочных электромагнитных излучений и наводок (ПК-13)
- 

### Содержание дисциплины

---

Раздел 1. Классификация, конструкции и параметры направляющих сред электросвязи  
Классификация направляющих сред электросвязи. Электрические и оптические направляющие среды. Конструкции и параметры кабельных линий связи. Конструкция электрических и оптических кабелей связи. Маркировка кабелей связи.

#### Раздел 2. Физические процессы в электрических направляющих средах

Эквивалентная схема двухпроводной цепи. Первичные параметры передачи, зависимость от частоты и конструкции. Телеграфные уравнения. Вторичные параметры передачи. Зависимость вторичных параметров от частоты и конструкции

#### Раздел 3. Взаимные влияния в кабельных цепях

Классификация взаимных влияний. Непосредственные и косвенные влияния. Регулярные и нерегулярные составляющие влияния. Нормирование взаимных влияний в направляющих

системах связи. Первичные параметры взаимных влияний. Эквивалентные схемы взаимных влияний. Расчеты помех на ближнем и дальнем концах симметричной линии при непосредственном влиянии. Вторичные параметры взаимных влияний, их зависимость от частоты и длины линии. Взаимные влияния между коаксиальными кабельными цепями. Сопротивление связи. Расчет помех. Вторичные параметры взаимных влияний, их зависимость от частоты и длины линии.

#### Раздел 4. Защита сооружений связи от взаимных и внешних электромагнитных влияний

Способы защиты линий связи от взаимных влияний. Скрутка цепей симметричных кабелей. Скрещивание симметричных цепей воздушных и кабельных линий связи. Схемы и индексы скрещивания. Симметрирование кабельных цепей. Экранирование кабельных цепей. Реакция экрана. Схемы организации связи: двухпроводная (одно- и двухчастотная) и четырехпроводная; однокабельная и двухкабельная. Источники опасных и мешающих внешних влияний. Нормы внешних влияний. Расчет опасных и мешающих внешних влияний. Меры защиты от опасных и мешающих влияний, применяемые на линиях связи. Устройство заземлений. Экранирование кабелей связи. Экранное затухание цилиндрического экрана для электрического, магнитного и электромагнитного полей, его зависимость от частоты и конструкции. Преимущества многослойных экранов. Виды коррозии. Меры защиты от коррозии, применяемые на установках сильного тока и установках связи.

#### Раздел 5. Защита сооружений связи от коррозии

Причины, виды и классификация коррозии. Коррозия блуждающими токами электрифицированных железных дорог и трамвайных сетей. Методы определения потенциалов и токов на оболочке кабеля, находящегося в зоне блуждающего тока. Методы электрических измерений. Почвенная коррозия и межкристаллитная коррозия.

#### Раздел 6. Измерения электрических линейных трактов, локализация неоднородностей и повреждений

Классификация измерений. Причины и классификация повреждений в электрических кабелях связи. Профилактические измерения на электрических кабельных линиях. Аварийные измерения на электрических кабельных линиях. Измерения на постоянном и переменном токе, импульсные (рефлектометрические) измерения. Нормы на параметры кабельных цепей.

#### Раздел 7. Физические процессы в оптических направляющих средах

Законы отражения и преломления света. Распространение света в многомодовых и одномодовых оптических волокнах. Нормированная частота. Длина волны отсечки. Коэффициент затухания и его зависимость от длины волны. Виды дисперсии. Межмодовая дисперсия, ее зависимость от профиля показателя преломления. Оптимальный профиль показателя преломления. Расчет уширения оптического импульса в многомодовом волокне. Хроматическая дисперсия. Зависимость от профиля показателя преломления и длины волны. Длина волны нулевой дисперсии. Расчет уширения оптического импульса в одномодовом волокне. Поляризационно-модовая дисперсия.

#### Раздел 8. Измерения оптических линейных трактов, локализация неоднородностей и повреждений

Классификация измерений. Причины и классификация повреждений в оптических кабелях связи. Профилактические измерения на оптических кабельных линиях. Аварийные измерения на оптических кабельных линиях. Измерения в проходящем и рассеянном свете. Рефлектометрия. Нормы на параметры оптических волокон.

#### Раздел 9. Волоконно-оптические системы связи и защита информации

Утечка информации и каналы утечки. Структура канала утечки информации. Технологии несанкционированного доступа к ОВ. Разрывный способ. Безразрывный способ без

принудительного отвода мощности. Безразрывный с принудительным отводом мощности. Формирование каналов утечки внешним воздействием- изгиб волокна. Формирование каналов утечки внешним воздействием, вызывающим изменением отношения показателей преломления. Формирование каналов утечки внешним воздействием без изменения формы волокна (сдавливание, растяжение). Формирование каналов утечки методом оптического туннелирования. Методы диагностики и противодействия НСД. Система диагностики по коэффициенту ошибок. ВОЛП с рефлектометрическими системами диагностики состояния ВОЛТ.

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

### **Б1.В.09 Основы стеганографии**

Цели освоения дисциплины

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

Место дисциплины в структуре ОП

Дисциплина «Основы стеганографии» Б1.В.11 является дисциплиной части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Изучение дисциплины «Основы стеганографии» опирается на знания дисциплин(ы) «Криптографические протоколы».

Требования к результатам освоения

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

- Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности; (ОПК-9)
- Способен противодействовать угрозам безопасности информации с использованием встроенных средств защиты информации операционных систем (ПК-3)

#### Содержание дисциплины

##### Раздел 1. Области применения стеганографии

Определение цифровой стеганографии (СГ) в широком смысле. Собственно СГ и цифровые "водяные" знаки (ЦВЗ). Типичные покрывающие сообщения (ПС). Основные атаки на системы СГ и ЦВЗ.

##### Раздел 2. Простейшие системы СГ

Вложение в наименьшие значащие биты (НЗБ) с замещением и НЗБ с согласованием. Основные свойства СГ-НЗБ. Примеры систем с НЗБ (Jsteg, Outgiess, F5). СГ, использующие широкополосные сигналы (СГ-ШПС) и их свойства. Слепой и информированный декодеры.

##### Раздел 3. СГ для других покрывающих сообщений

Лингвистические, графические, Интернет СГ и их свойства.

##### Раздел 4. СГ стойкие к оптимальному статистическому обнаружению

Критерии секретности СГ. Относительная энтропия. Модельно обусловленные СГ. СГ на основе адаптивного квантования. СГ с сохранением статистики ПС. Слепой стегоанализ.

##### Раздел 5. Общие сведения о системах с ЦВЗ

Классификация систем ЦВЗ. Основные атаки на системы ЦВЗ. Критерии эффективности ЦВЗ. Виды ПС использующихся с ЦВЗ. Основные применения систем ЦВЗ

##### Раздел 6. Техника погружения и извлечения ЦВЗ устойчивых к случайному и преднамеренному удалению

Классификация систем ЦВЗ. Основные атаки на системы ЦВЗ. Критерии эффективности ЦВЗ. Виды ПС использующихся с ЦВЗ. Основные применения систем ЦВЗ (мониторинг рекламы, идентификация пользователей доказательство прав собственности, аутентификация ПС).

##### Раздел 7. Особенности построения систем ЦВЗ для аудио и видео сигналов

ЦВЗ на основе использования явлений эхо и реверберации. Применение кепстральных методов в декодере. Защита от преобразований форматов. Основные методы построения систем ЦВЗ для видео ПС различных стандартов.

#### Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

#### Форма промежуточной аттестации

Зачет

### **Б1.В.10 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.10 является дисциплиной части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки бакалавриата по направлению «10.03.01 Информационная безопасность». Изучение дисциплины «Защита информации в центрах обработки данных» опирается на знания дисциплин(ы) «Безопасность Astra-Linux»; «Защита в операционных системах».

---

#### Требования к результатам освоения

---

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

- Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности; (ОПК-8)
- Способен проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах (ПК-5)

---

#### Содержание дисциплины

---

##### Раздел 1. Введение в центры обработки данных (ЦОД)

Понятие центра обработки данных, структура ЦОД

##### Раздел 2. Виртуализация и ЦОД

Настройка виртуальных машин, клонирование и создание шаблонов VM

##### 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 (НА)

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

180 час(ов), 5 ЗЕТ

Форма промежуточной аттестации

Экзамен

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

---

Цели освоения дисциплины

Целью преподавания дисциплины «Безопасность беспроводных локальных сетей» является:

изучение архитектуры, структуры, функции, компонентов беспроводных локальных сетей

---

Место дисциплины в структуре ОП

Дисциплина «Безопасность беспроводных локальных сетей» Б1.В.ДВ.01.01 является дисциплиной по выбору части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки 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:

- Способен настраивать правила фильтрации пакетов в компьютерных сетях (ПК-7)
- Способен конфигурировать и контролировать корректность настройки программно-аппаратных средств защиты информации в компьютерных сетях (ПК-8)

---

Содержание дисциплины

Раздел 1. Введение в беспроводные сети стандарта IEEE 802.11

IEEE 802.11 — набор стандартов связи для коммуникации в беспроводной локальной сетевой зоне частотных диапазонов 0,9, 2,4, 3,6 и 5 ГГц.

Раздел 2. Основные принципы радиоанализа и радиопланирования

Принципы распределения радиоволн, виды антенн, расчет допустимой мощности.

Раздел 3. Основы и принципы работы протокола RADIUS, DIAMETER, семейство протоколов EAP

Протоколы RADIUS, DIAMETER, семейство протоколов EAP.

Раздел 4. Стандарт IEEE 802.1x, технологии профилирования в беспроводных сетях стандарта IEEE 802.11

IEEE 802.1x - стандарт аутентификации пользователей в сети.

Раздел 5. Технологии динамического изменения авторизации

Настройка динамического изменения авторизации

Раздел 6. Администрирование интерфейса конечных пользователей

Администрирование интерфейса конечных пользователей в системе Cisco UC

Раздел 7. Возможности телефонии и мобильности, и поддержка решения Cisco UC

Настройка возможностей телефонии и мобильности, поддержка решения Cisco UC

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет. Курсовая работа

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

Цели освоения дисциплины

Целью преподавания дисциплины «Защищенные мобильные приложения» является:

изучение основных проблем, возникающих при разработке приложений для мобильных устройств, а также получение представления о проблемах, стоящих перед разработчиком таких приложений.

Место дисциплины в структуре ОП

Дисциплина «Защищенные мобильные приложения» Б1.В.ДВ.01.02 является дисциплиной по выбору части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки 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:

- Способен настраивать правила фильтрации пакетов в компьютерных сетях (ПК-7)
  - Способен конфигурировать и контролировать корректность настройки программно-аппаратных средств защиты информации в компьютерных сетях (ПК-8)
- 

Содержание дисциплины

---

Раздел 1. Обзор мобильных платформ

Обзор мобильных платформ

Раздел 2. Работа с приложениями

Создание приложений. Реализация интерфейсов. Управление ресурсами. Хранение информации. Доступ с аппаратными возможностями

Раздел 3. Изучение структуры защищенных мобильных приложений

Просмотр исходного кода, постановка требований на доработку. Дополнительные задания

---

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет. Курсовая работа

---

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

Цели освоения дисциплины

---

Целью преподавания дисциплины «Безопасность IP-телефонии» является: изучение архитектуры, настройки IP-телефонии. Знакомство с протоколами, обеспечивающими передачу данных в реальном времени – RTP, RTCP и сигнализационными протоколами SIP, MGCP, H.323

---

Место дисциплины в структуре ОП

---

Дисциплина «Безопасность IP-телефонии» Б1.В.ДВ.02.01 является дисциплиной по выбору части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки 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:

- Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты; (ОПК-10)
  - Способен проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах (ПК-5)
  - Способен оценивать угрозы безопасности информации в компьютерных сетях (ПК-6)
- 

## Содержание дисциплины

---

### Раздел 1. Введение

Предмет и основные задачи дисциплины «Безопасность IP-телефонии», её значение в сис-теме подготовке бакалавров по направлению «Инфокоммуникационные технологии и системы связи»

### Раздел 2. Кодеки, используемые в IP-телефонии. Цифровой сигнальный процессор (DSP).

Классификация VoIP кодеков. Типы цифровых сигнальных процессоров. Расчет требуемой полосы пропускания в зависимости от вида кодека. Настройка DSP.

### Раздел 3. Сигнализация в VoIPсетях. Рекомендации H.323. Протоколы SIP и SDP

Протоколы сигнализации H.323, Session Initiation Protocol (SIP), MGCP протокол. Стадии обработки голосового трафика. Компоненты VoIP. Квантование. Сэмплирование.

### 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), негарантированной доставки (BestEffort). Механизмы обеспечения качества обслуживания в сетях передачи голоса: маркировка, приоритизация, 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

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

#### Цели освоения дисциплины

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

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

#### Место дисциплины в структуре ОП

Дисциплина «Защита multicast трафика в сети Интернет» Б1.В.ДВ.02.02 является дисциплиной по выбору части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки 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 операционных систем сетевых устройств».

#### Требования к результатам освоения

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

- Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты; (ОПК-10)
- Способен проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах (ПК-5)
- Способен оценивать угрозы безопасности информации в компьютерных сетях (ПК-6)

#### Содержание дисциплины

##### Раздел 1. Раздел 1. Введение

Предмет и основные задачи дисциплины «Защита голосового трафика в сети Интернет», её значение в системе подготовки бакалавров по направлению «Инфокоммуникационные технологии и системы связи».

Раздел 2. Раздел 2. Кодеки, используемые в IP-телефонии. Цифровой сигнальный процессор (DSP).

Классификация VoIP кодеков. Типы цифровых сигнальных процессоров. Расчет требуемой полосы пропускания в зависимости от вида кодека. Настройка DSP.

Раздел 3. Раздел 3. Сигнализация в VoIP-сетях. Рекомендации H.323. Протоколы SIP и SDP.  
Протоколы сигнализации H.323, Session Initiation Protocol (SIP), MGCP протокол. Стадии обработки голосового трафика. Компоненты VoIP. Квантование. Сэмплирование.

Раздел 4. 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. Раздел 5. Механизмы обеспечения QoS для VoIP.  
Обзор моделей качества обслуживания (QoS): дифференцированного обслуживания (DiffServ), интегрированного сервиса (IntServ), негарантированной доставки (BestEffort). Механизмы обеспечения качества обслуживания в сетях передачи голоса: маркировка, приоритизация, полисинг, шейпинг трафика. CiscoAutoQoS.

Раздел 6. Раздел 6. Введение в CUCM Express.  
Настройка CUCM Express на маршрутизаторе Cisco, функции CUCM Express в голосовой среде.

Раздел 7. Раздел 7. Пограничные контроллеры сессий (SBC).  
Механизмы защиты голосового трафика: конфиденциальность, целостность, аутентификация. Протокол Secure RTP. Алгоритмы шифрования: DES, 3DES, AES. Защита от распределенных атак обслуживания (DDoS).

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

### ***Б1.В.ДВ.03.01 Противодействие техническим средствам разведки***

Цели освоения дисциплины

Целью преподавания дисциплины «Противодействие техническим средствам разведки» является:

Роль противодействия техническим средствам разведки в условиях взаимодействия сложных систем различного уровня определяется его вкладом в достижение превосходства в сфере управления. Роль противодействия техническим средствам разведки в условиях конфликтного взаимодействия сложных систем различного уровня определяется его вкладом в достижение превосходства в сфере управления.

Место дисциплины в структуре ОП

Дисциплина «Противодействие техническим средствам разведки» Б1.В.ДВ.03.01 является дисциплиной по выбору части, формируемой участниками

образовательных отношений 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:

- Способен проводить работы по установке, настройке, испытаниям и техническому обслуживанию средств защиты информации от утечки по техническим каналам; (ОПК-3,1)
- Способен проводить контроль эффективности защиты информации от утечки по техническим каналам; (ОПК-3,3)
- Способен проводить работы по установке, настройке и испытаниям защищенных технических средств обработки информации (ПК-12)

---

#### Содержание дисциплины

---

##### Раздел 1. Обнаружение и анализ демаскирующих признаков

Противодействие обнаружению демаскирующих признаков. Противодействие анализу демаскирующих признаков.

##### Раздел 2. Главные направления снижения эффективности ТСР

Противодействие обнаружению демаскирующих признаков преследуется цель скрытия демаскирующих признаков от ТСР.

##### Раздел 3. Организация противодействие техническим средствам разведки (ПД ТСР)

Организация работы по анализу внутренних и внешних угроз (в том числе выработка мер по обеспечению ее защиты). Организация использования технических средств (в том числе сбора, обработки, накопления и хранения конфиденциальной информации).

##### Раздел 4. Служба безопасности

Изучение, анализ и оценка состояния обеспечения экономической и информационной безопасности предприятия и разработка предложений и рекомендаций для их совершенствования. Разработка технико-экономических обоснований, направленных на приобретение технических средств, получение консультации у специалистов, разработку необходимой документации в целях совершенствования системы мер по обеспечению экономической и информационной безопасности.

---

#### Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

#### Форма промежуточной аттестации

Зачет

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

### Цели освоения дисциплины

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

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

### Место дисциплины в структуре ОП

Дисциплина «Основы криптографии с открытым ключом» Б1.В.ДВ.03.02 является дисциплиной по выбору части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки 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:

- Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности; (ОПК-9)
- Способен противодействовать угрозам безопасности информации с использованием встроенных средств защиты информации операционных систем (ПК-3)

### Содержание дисциплины

#### Раздел 1. Математический базис криптосистем с открытым ключом

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-Гамала, РША, Рабина, Мас-Элис. Генерирование ключей, шифрование, дешифрование. Атаки на криптосистемы.

#### Раздел 3. Системы электронной цифровой подписи

Построение криптосистем на основе эллиптических кривых. Бесключевые хэш-функции.

Модель электронной цифровой подписи сообщения, виды ЭЦП. ЭЦП на основе различных криптосистем. Стандарты ЭЦП и хэш-функции.

#### Раздел 4. Криптографические протоколы

Обзор основных протоколов. Изучение протоколов разделения секрета, аутентификация пользователей с нулевым разглашением, секретные совместные вычисления, тайное голосование.

#### Раздел 5. Управление открытыми ключами

Принцип построения инфраструктуры открытых ключей (PKI), назначение и использование сертификатов открытых ключей. Распределение ключей для симметричных систем на основе криптографии с открытыми ключами.

---

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

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

---

Цели освоения дисциплины

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

Целью преподавания дисциплины является изучение вопросов защиты операционных систем.

---

Место дисциплины в структуре ОП

---

Дисциплина «Защита операционных систем сетевых устройств» Б1.В.ДВ.04.01 является дисциплиной по выбору части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки 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:

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

---

## Содержание дисциплины

---

### Раздел 1. История развития операционных систем

История разработки ОС MSDOS, Windows и 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 GNU/Linux.

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 GNU/Linux для ограничений доступа к сервисам. Ведение системного журнала.

### Раздел 3. Основы управление доступом в ОС GNU/Linux.

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-Enhanced Linux. Управление моделью безопасности SELinux: моды, контексты. Описание прав доступа к файлам и процессам.

### Раздел 5. Контроль сетевого трафика в ОС GNU/Linux.

Описано семейство протоколов TCP/IP и их реализация в GNU/Linux, обосновано разделение сетевых протоколов на уровни и выделены задачи, решаемые на каждом из них. Приведены утилиты GNU/Linux для работы с сетью. Алгоритм обработки сетевого трафика. Настройка межсетевого экрана ОС GNU/Linux. Создание правил фильтрации трафика. Применение механизма SELinux к обработке IP-пакетов.

### Раздел 6. Система управления доступом в ОС MSWindows.

Основные компоненты ОС MSWindows. Модель операционной системы. Различия между клиентской и серверной версии. Системные процессы, драйвера, ядро. Вводится понятие реестр операционной системы. Управление сервисами и процессами. Система журналирования.

### Раздел 7. Роли ОС MSWindows 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 8. Управление пользователями, группами и назначением прав доступа с использованием ActiveDirectory.



Контроль учетных записей, разрешения для файлов и папок, блокировка учетной записи и политики паролей, детальные политики паролей, возможности аудита, функции шифрования данных. Обеспечение безопасности файлов и папок. Аудит файлов. Шифрование файлов.

Раздел 9. Реализация системы безопасности сети в ОС MSWindows.

Утилиты по настройке сети. Угрозы сетевой безопасности, реализация брандмауэров. Настройка брандмауэра Windows. Защита доступа к сети.

Раздел 10. Внедрение программ обеспечения безопасности в ОС MSWindows.

Установка дополнительной системы защиты информации, для упрощения управлением доступом к файлам, на примере системы SearchInform.

---

Общая трудоемкость дисциплины

216 час(ов), 6 ЗЕТ

Форма промежуточной аттестации

Экзамен

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

---

Цели освоения дисциплины

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

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

---

Место дисциплины в структуре ОП

Дисциплина «Защита информации с помощью маршрутизаторов и коммутаторов» Б1.В.ДВ.04.02 является дисциплиной по выбору части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки 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 «Основы маршрутизации в компьютерных сетях».

---

Требования к результатам освоения

---

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

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

Содержание дисциплины

---

### Раздел 1. Введение

Предмет и основные задачи дисциплины «Защита информации с помощью маршрутизаторов и коммутаторов», её значение в системе подготовки 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 асимметричная криптография. Виды VPN. Внедрение виртуальных частных сетей на маршрутизаторе, используя виртуальные туннельные интерфейсы (VTI).

### Раздел 6. Использование цифровых сертификатов для обеспечения масштабируемой аутентификации VPN (PKI).

Понятие цифровых сертификатов. Применение алгоритмов асимметричной 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

216 час(ов), 6 ЗЕТ

Форма промежуточной аттестации

Экзамен

---

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

Цели освоения дисциплины

---

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

---

Место дисциплины в структуре ОП

---

Дисциплина «Общая физическая подготовка» Б1.В.ДВ.10.01 является дисциплиной по выбору вариативной 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:

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

---

Содержание дисциплины

---

Раздел 1. Методика проведения учебно-тренировочного занятия.

Оценка двигательной активности и суточных энергетических затрат. Базовый комплекс упражнений общей физической подготовки. Использование подвижных, спортивных игр.

Раздел 2. Овладение двигательными навыками и методами проведения занятий по общей физической подготовки.

Методика самооценки уровня и динамики общей и специальной физической подготовленности. Ознакомление и обучение двигательным навыкам на занятиях общей физической подготовки. Базовый комплекс упражнений общей физической подготовки. Раздел 3. Повышение уровня функциональных и двигательных способностей, направленного формирования качеств и свойств личности.

Методы самоконтроля здоровья, физического развития и функциональной подготовленности. Комплексное занятие: упражнения для развития гибкости, выносливости, силы, быстроты и ловкости. Использование подвижных, спортивных игр. Раздел 4. Овладение методами и способами физкультурно-спортивной деятельности.

Средства и методы мышечной релаксации в спорте. Методы спортивной тренировки. Комплексное занятие: упражнения для развития основных физических качеств. Раздел 5. Направленное развитие основных физических качеств. Подготовка к сдаче нормативов ГТО.

Методики самостоятельного освоения отдельных элементов профессионально-прикладной физической подготовки (ППФП). Комплексное занятие: упражнения для развития основных физических качеств. Подготовка к выполнению тестовых испытаний и сдаче нормативов ГТО.

Раздел 6. Приобретение опыта практической деятельности, повышения уровня функциональных и двигательных способностей.

Комплексное занятие: упражнения для развития основных физических качеств. Использование подвижных, спортивных игр.

---

Общая трудоемкость дисциплины

328 час(ов),

Форма промежуточной аттестации

Зачет

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

Цели освоения дисциплины

---

Целью преподавания дисциплины «Адаптационная физическая подготовка» является:

максимально возможное развитие жизнеспособности человека, имеющего отклонения в состоянии здоровья и обеспечение оптимального режима функционирования двигательных возможностей, духовных сил, их гармонизацию для самореализации в качестве социально и индивидуально значимого субъекта.

---

Место дисциплины в структуре ОП

---

Дисциплина «Адаптационная физическая подготовка» Б1.В.ДВ.10.02 является дисциплиной по выбору вариативной 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:

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

---

#### Содержание дисциплины

---

##### Раздел 1. Методика проведения учебно-тренировочного занятия.

Оценка двигательной активности и суточных энергетических затрат. Базовый комплекс упражнений общей физической подготовки. Использование подвижных, спортивных игр (по упрощенным правилам).

##### Раздел 2. Овладение двигательными навыками и методами проведения занятий по общей физической подготовке.

Методика самооценки уровня и динамики общей и специальной физической подготовленности. Ознакомление и обучение двигательным навыкам, на занятиях общей физической подготовки. Базовый комплекс упражнений общей физической подготовки.

##### Раздел 3. Повышение уровня функциональных и двигательных способностей, направленного формирования качеств и свойств личности.

Методы самоконтроля здоровья, физического развития и функциональной подготовленности. Комплексное занятие: упражнения для развития гибкости, выносливости (адаптивные формы), силы (адаптивные формы), быстроты и ловкости. Использование подвижных, спортивных игр (по упрощенным правилам).

##### Раздел 4. Овладение методами и способами физкультурно-спортивной деятельности.

Средства и методы мышечной релаксации в спорте. Методы спортивной тренировки. Комплексное занятие: упражнения для развития основных физических качеств (адаптивные формы).

##### Раздел 5. Развитие физических качеств и совершенствование координационных способностей.

Методики самостоятельного освоения отдельных элементов профессионально-прикладной физической подготовки. Комплексное занятие: упражнения для развития основных физических качеств (адаптивные формы). Использование подвижных, спортивных игр (адаптивные формы). Подготовка к выполнению тестовых испытаний, доступных по медицинским показаниям.

##### Раздел 6. Приобретение опыта практической деятельности, повышение уровня функциональных и двигательных способностей.

Комплексное занятие: упражнения для развития основных физических качеств (адаптивные формы). Использование подвижных, спортивных игр (по упрощенным правилам).

---

Общая трудоемкость дисциплины

328 час(ов),

Форма промежуточной аттестации

Зачет

---

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

---

Цели освоения дисциплины

Целью преподавания дисциплины «Секции по видам спорта» является:

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.05.03 является дисциплиной по выбору части, формируемой участниками образовательных отношений 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:

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

---

Содержание дисциплины

---

Раздел 1. Методика проведения учебно-тренировочного занятия.

Оценка двигательной активности и суточных энергетических затрат. Комплексное занятие: упражнения для развития гибкости, выносливости, силы, быстроты и ловкости.

---

Раздел 2. Овладение двигательными навыками, техническими приемами, индивидуальной и групповой тактики в избранном виде спорта.

Методика самооценки уровня и динамики общей и специальной физической подготовленности. 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**

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

Цели проведения практики

---

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

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

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

---

Место практики в структуре ОП

---

«Эксплуатационная практика» Б2.В.01.01(П) входит в блок 2 учебного плана, который относится к части, формируемой участниками образовательных отношений, и является обязательной составной частью образовательной программы по направлению «10.03.01 Информационная безопасность».

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

---

Требования к результатам освоения

---

В процессе прохождения практики студент формирует и демонстрирует следующие компетенции:

- Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности; (ОПК-8)
- Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты; (ОПК-10)
- Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений; (ОПК-12)
- Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач (УК-1)
- Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(ых) языке(ах) (УК-4)
- Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни (УК-6)

---

Содержание практики



---

Раздел 1. Согласование темы индивидуального задания

Выбор и согласование темы с научным руководителем

Раздел 2. Составление индивидуального плана работы студента

Определение и согласование индивидуального плана работы

Раздел 3. Выполнение индивидуального задания

Получение и выполнение индивидуального задания

Раздел 4. Подготовка отчета

Оформление и подготовка работы

Раздел 5. Защита отчета

Выступление и защита работы

---

Общая трудоемкость дисциплины

324 час(ов), 9 ЗЕТ

Форма промежуточной аттестации

Зачет

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

Цели проведения практики

---

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

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

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

Место практики в структуре ОП

---

«Ознакомительная практика» Б2.О.01.01(У) входит в блок 2 учебного плана, который относится к обязательной части, и является обязательной составной частью образовательной программы по направлению «10.03.01 Информационная безопасность».

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

---

#### Требования к результатам освоения

---

В процессе прохождения практики студент формирует и демонстрирует следующие компетенции:

- Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности; (ОПК-2)
- Способен проводить эксперименты по заданной методике и обработку их результатов; (ОПК-11)
- Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни (УК-6)

---

#### Содержание практики

---

##### Раздел 1. Согласование темы индивидуального задания

Выбор и согласование темы с научным руководителем

##### Раздел 2. Составление индивидуального плана работы студента

определение и согласование индивидуального плана работы

##### Раздел 3. Выполнение индивидуального задания

получение и выполнение индивидуального задания

##### Раздел 4. Подготовка отчета

оформление и подготовка работы

##### Раздел 5. Защита отчета

выступление и защита работы

---

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

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

### Цели проведения практики

---

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

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

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

### Место практики в структуре ОП

---

«Преддипломная практика» Б2.О.02.01(Пд) входит в блок 2 учебного плана, который относится к обязательной части, и является обязательной составной частью образовательной программы по направлению «10.03.01 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:

- Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности; (ОПК-8)
- Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты; (ОПК-10)
- Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений; (ОПК-12)
- Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач (УК-1)
- Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(ых) языке(ах) (УК-4)
- Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни (УК-6)

---

#### Содержание практики

---

##### Раздел 1. Согласование темы индивидуального задания

Выбор и согласование темы с научным руководителем

##### Раздел 2. Составление индивидуального плана работы студента

определение и согласование индивидуального плана работы

##### Раздел 3. Выполнение индивидуального задания

получение и выполнение индивидуального задания

##### Раздел 4. Подготовка отчета

оформление и подготовка работы

##### Раздел 5. Защита отчета

выступление и защита работы

---

Общая трудоемкость дисциплины

324 час(ов), 9 ЗЕТ

Форма промежуточной аттестации

Зачет

#### **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 следующие виды деятельности:

- эксплуатационный
- проектно-технологический
- экспериментально-исследовательский
- организационно-управленческий.

---

### Место дисциплины в структуре ОП

---

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

---

### Требования к результатам освоения

---

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

В соответствии с ФГОС:

- Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства; (ОПК-1)
- Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности; (ОПК-2)
- Способен использовать необходимые математические методы для решения задач профессиональной деятельности; (ОПК-3)
- Способен проводить работы по установке, настройке, испытаниям и техническому обслуживанию средств защиты информации от утечки по техническим каналам; (ОПК-3.1)
- Способен проводить работы по установке, настройке, испытаниям и техническому обслуживанию средств защиты информации от несанкционированного доступа; (ОПК-3.2)
- Способен проводить контроль эффективности защиты информации от утечки по техническим каналам; (ОПК-3.3)
- Способен проводить контроль защищенности информации от несанкционированного доступа; (ОПК-3.4)
- Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности; (ОПК-4)
- Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности; (ОПК-5)

- Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю; (ОПК-6)
- Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности; (ОПК-7)
- Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности; (ОПК-8)
- Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности; (ОПК-9)
- Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты; (ОПК-10)
- Способен проводить эксперименты по заданной методике и обработку их результатов; (ОПК-11)
- Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений; (ОПК-12)
- Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма (ОПК-13)
- Способен формулировать и настраивать политики безопасности операционных систем (ПК-1)
- Способен оценивать угрозы безопасности информации операционных систем (ПК-2)
- Способен противодействовать угрозам безопасности информации с использованием встроенных средств защиты информации операционных систем (ПК-3)
- Способен устанавливать и настраивать антивирусные средства защиты информации в операционных системах (ПК-4)
- Способен проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах (ПК-5)
- Способен оценивать угрозы безопасности информации в компьютерных сетях (ПК-6)
- Способен настраивать правила фильтрации пакетов в компьютерных сетях (ПК-7)
- Способен конфигурировать и контролировать корректность настройки программно-аппаратных средств защиты информации в компьютерных сетях (ПК-8)
- Способен анализировать угрозы безопасности информации программного обеспечения (ПК-9)
- Способен формулировать и обосновывать правила безопасной эксплуатации программного обеспечения (ПК-10)
- Способен осуществлять мероприятия по противодействию угрозам безопасности информации, возникающим при эксплуатации программного обеспечения (ПК-11)
- Способен проводить работы по установке, настройке и испытаниям защищенных технических средств обработки информации (ПК-12)
- Способен проводить контроль эффективности защиты информации от утечки за счет побочных электромагнитных излучений и наводок (ПК-13)
- Способен проводить контроль эффективности защиты акустической (речевой) информации от утечки по техническим каналам (ПК-14)
- Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач (УК-1)
- Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений (УК-2)

- Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде (УК-3)
- Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(ых) языке(ах) (УК-4)
- Способен воспринимать межкультурное разнообразие общества в социально-историческом, этическом и философском контекстах (УК-5)
- Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни (УК-6)
- Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности (УК-7)
- Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов (УК-8)
- Способен принимать обоснованные экономические решения в различных областях жизнедеятельности (УК-9)
- Способен формировать нетерпимое отношение к коррупционному поведению (УК-10)

---

Содержание

---

Подготовка и защита выпускной квалификационной работы

---

Общая трудоемкость дисциплины

216 час(ов), 6 ЗЕТ