АННОТАЦИЯ ДИСЦИПЛИНЫ
С1.Б.1 «ИСТОРИЯ ОТЕЧЕСТВА»

ТРУДОЕМКОСТЬ ЗЕТ 4 (144 ЧАСА)

1. ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью изучения дисциплины является – изучение важнейших процессов общественно-политического развития России с древнейших времен до наших дней на фоне истории мировой цивилизации;

Для достижения цели ставятся задачи:

- определение места России в мировой цивилизации;
- изучение исторического пути Российского государства, познание и характеристика всех его сторон, явлений, событий и фактов;
- определение роли выдающихся исторических деятелей, их влияния на ход российской истории;
- выработка у студентов основ логического мышления и навыков причинно-следственного анализа исторического процесса;
- формирование у студентов научного мировоззрения;
- помощь студентам в выработке объективной позиции по вопросам, касающимся ценностного отношения к историческому прошлому.

2. КОМПЕТЕНЦИИ, ПРИОБРЕТАЕМЫЕ СТУДЕНТОМ В ПРОЦЕССЕ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ ОК-3, ОК-4, ОК-10,

3. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ

3.1. Студент должен знать:

- основные события и процессы Отечественной истории, специфику исторических закономерностей;
- осознавать место и роль России в мировой истории и в современном мире;
- четко для себя представлять базовые ценности Отечественной истории и культуры;
- основные положения и методы социальных, гуманитарных и экономических наук.

3.2 Студент должен уметь:

- определять свою гражданскую позицию;
- логически верно, аргументировано и ясно строить устную и письменную речь;
- теоретически обобщать факты, выявлять проблемы, причинно-следственные связи, закономерности и главные тенденции развития исторического процесса
- работать с приборами и оборудованием в современной лаборатории;
- использовать различные методики физических измерений и обработки экспериментальных данных;
- использовать сравнительно-исторический и хронологический методы, а также применять методы исторического анализа к решению конкретных естественнонаучных и гуманитарных проблем.

3.3. Студент должен владеть:

- навыками анализа исторических фактов и использования исторических знаний для прогнозирования современной социально-экономической и политической ситуации;

- навыками всесторонней и объективной оценки исторических событий и процессов;

- основными методами работы с историческими источниками, навыками работы с информацией в глобальных компьютерных сетях;

- навыками обработки и интерпретирования результатов эксперимента;

- навыками использования методов физического моделирования в производственной практике.

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ. ОСНОВНЫЕ РАЗДЕЛЫ

Шифр дисциплины	Наименование разделов и содержание дисциплины	Всего часов(Зачёт
1	2	3
Б1.В.ОД.1	ОТЕЧЕСТВЕННАЯ ИСТОРИЯ	72 (2)
	Великое переселение народов. Происхождение славян. Восточные славяне в IV-IX вв. Образование Древнерусского государства. Норманнская теория. Древняя Русь и кочевники. Византийско-древнерусские связи. Особенности социального строя Древней Руси. Принятие христианства. Эволюция восточнославянской государственности в XI-XII вв. Формирование русского централизованного государства. Экономические, политические факторы и их влияние на объединение русских земель. Роль московских князей в объединении. Социально-политические изменения в русских землях в XIII-XV вв. Русь и средневековые государства Европы и Азии. Специфика формирования единого Российского государства. Возвышение Москвы. Политика Ивана III, Василия III, Ивана IV. Предпосылки и особенности складывания российского абсолютизма. Особенности экономического, политического и культурного развития России на рубеже XVII-XVIII вв. Преобразовательная деятельность Петра I и ее результаты. Политика «просвещенного абсолютизма» в России. Особенности и основные этапы экономического развития России. Эволюция форм собственности на землю. Структура феодального землевладения. Крепостное право в России. Особенности развития России в первой половине XIX в. Отечественная война 1812 г. Промышленная революция в России: общее и особенное. Объективная необходимость	

	отмены крепостного права. Общественная мысль и общественные движения России в XIX веке. Буржуазные реформы 60-70-х гг. XIX века. Роль XX столетия в мировой истории. Глобализация общественных процессов. Россия в начале XX века. Революция 1905-1907 гг. Столыпинские реформы. Россия в условиях мировой войны и общенационального кризиса. Февраль 1917 г. Октябрьские события 1917 г. Второй Всероссийский съезд Советов и установление Советской власти по всей стране. Первые социально-экономические и политические преобразования в советской России. Социально-экономическое развитие страны в 1920-е гг. Переход к НЭПу и его первые результаты. Образование СССР. Социально-экономические и культурные преобразования в 1930-е гг. Создание общества «государственного социализма». СССР накануне и в начальный период Второй мировой войны. Великая Отечественная война. Мобилизация сил страны на разгром врага. Социально-экономическое развитие, общественно-политическая, культура СССР в послевоенный период (1946-1953). Приход к власти Н.С. Хрущева. Десталинизация как начало демократизации советского общества. Научно-техническая политика СССР в условиях НТР. Экономика, социальная сфера, наука и культура в конце 50-х – первой половине 60-х гг. Система «коллективного руководства» Л.И. Брежнева и нарастание кризисных явлений в партийно-государственной системе. Экономическая реформа 1965 г. Непоследовательность ее осуществления и усиление командно-административных методов в экономической политике 1970-х гг. Перестройка в СССР. М.С. Горбачев и поворот в развитии страны. Гласность как элемент демократизации советского режима. Экономические реформы, их последствия, усиление кризисных явлений в стране в конце 1980-х гг. Распад СССР, образование СНГ. Становление новой российской государственности. Россия и мир в условиях перехода к постиндустриальной цивилизации. Новые явления в экономической, социальной и политической жизни.	

Аннотация к рабочей программе учебной дисциплины «Философия»

ТРУДОЕМКОСТЬ ЗЕТ 4 (144 ЧАСА)

Цель дисциплины: формирование и развитие у студентов познавательного интереса в области фундаментальных знаний по

конкретному направлению подготовки, а также знаний общенаучного характера; формирование общекультурных компетенций; приобретение знаний и умений, необходимых для осмысления основных тем философии и значения как ее методологической и мировоззренческой, так и аксиологической и гуманистической функций. В процессе изучения дисциплины у студентов должны быть сформированы основы научного мышления, в том числе: понимание принципов научного поиска, умение применять общенаучные методы исследования в предметной деятельности.

Задачи дисциплины:

-формирование и развитие у студентов философского мировоззрения как теоретической базы для построения целостного системного представления о мире и месте человека в нем;

-выработка навыков критической оценки философских и научных течений, направлений и школ, социальной информации;

-развитие умения правильно формулировать, излагать и аргументировано отстаивать собственное видение рассматриваемых проблем;

-способствование осмыслению мира как совокупности культурных достижений человеческого общества, становлению знаний о проблемах современной цивилизации в целом, науки и техники в частности, пониманию необходимости несения ответственности перед человечеством будущим профессионалом в процессе научной и производственной практики.

Требования к результатам освоения дисциплины:

Компетенции, формируемые в результате освоения дисциплины (общекультурные):

ОК-1, ОК-2, ОК-3, ОК-4, ОК-6, ОК-7, ОК-9, ОК-10, ОК-11, ПК-5

В результате освоения дисциплины студент должен:

знать:

- содержание и взаимосвязь основных принципов, законов, понятий и категорий гуманитарных, социальных и экономических наук (ОК-3);
- основные этапы развития философской мысли, основную проблематику и структуру философского знания (ОК-3);
- применять критический подход в оценке и анализе различных научных гипотез, концепций и теорий (ОК – 9)
- методы научного и философского исследования, способы их использования в профессиональной деятельности (ОК-9-) (ОК-10)

уметь:

- применять критический подход в оценке и анализе различных научных гипотез, концепций и теорий (ОК – 9); (ОК-10)
- использовать принципы, законы и методы гуманитарных, социальных и экономических наук для решения профессиональных задач (ОК-10)
- анализировать мировоззренческие, социально и личностно значимые философские проблемы (ОК-3),(ОК-10);
- использовать в профессиональной деятельности знание современных проблем философии (ОК-3).(ОК-10)

владеть:

- основными методами научного познания (ОК-10);
- навыками аргументированного изложения своей точки зрения, ведения дискуссии, полемики, культурой мышления (ОК-10);
-методами самостоятельного философского исследования научных проблем (ОК-9)

Содержание дисциплины:

Раздел 1.История философии.

Раздел 2. Систематическая философия (основные философские проблемы).

Аннотация программы учебной дисциплины С1.Б.3

С1.Б.3«Иностранный язык»

ТРУДОЕМКОСТЬ ЗЕТ 8 (288 ЧАСА)

Цели и задачи дисциплины:

Приобретение коммуникативной компетенции, позволяющей будущим специалистам ориентироваться в современном информационном поле и владеть элементарными навыками межкультурной профессиональной коммуникации; повышение уровня культуры, общего образования и кругозора будущего специалиста.

Задачи изучения дисциплины:

формирование и совершенствование навыков чтения и понимания оригинальной литературы на иностранном языке по избранной специальности; системное повторение грамматического материала с функциональной направленностью объяснения и иллюстрацией грамматических явлений лексикой по широкому профилю факультета; выработка у студентов приёмов и навыков аннотирования, реферирования и перевода текстов по специальности; ознакомление студентов с современной научной терминологией на иностранном языке и формирование базовых навыков говорения и аудирования на основе изученного материала; воспитание уважения к духовным ценностям разных стран и народов; развитие умения самостоятельно совершенствовать знания по иностранному языку.

Компетенции, приобретаемые студентом в процессе изучения дисциплины ОК-2, ОК-6, ОК-7, ОК-8, ОК-9, ОК-10, ПК-9

В результате изучения дисциплины студент должен:

знать:

Лексический и грамматический минимум в объеме, необходимом для раоты с текстами профессиональной направленности и осуществления коммуникации на иностранном языке

уметь:

читать и переводить научно-техническую литературу на иностранном языке по профессиональной тематике, правильно употреблять

терминологическую лексику в профессиональной речи;

владеть:

иностранным языком в объеме, необходимом для получения и изложения информации по профессиональной тематике, навыками общения на иностранном языке.

Аннотация дисциплины С1.Б.4
«Правовые основы обеспечения компьютерной безопасности»

ТРУДОЕМКОСТЬ ЗЕТ 4 (144 ЧАСА)

Цель дисциплины:

Овладение студентами теоретическими знаниями в области истории и теории государства и права, конституционного, гражданского, семейного, трудового, административного, уголовного и экологического права; формирование навыков применения норм права в профессиональной деятельности, в том числе основ правового регулирования отношений в информационной сфере, конституционных гарантий прав граждан на получение информации и механизма их реализации, понятий и видов защищаемой информации по законодательству РФ, системы защиты государственной тайны, основ правового регулирования отношений в области интеллектуальной собственности и способов защиты этой собственности, понятий и видов компьютерных преступлений

Задачи дисциплины:

- Ознакомить с основами российской правовой системы и законодательства, организацией судебных и иных правоприменительных и правоохранительных органов.
- Раскрыть права и свободы человека и гражданина, научить их реализовать в различных сферах жизнедеятельности.
- Научить использовать и составлять нормативные и правовые документы в области информационного законодательства Российской Федерации;
- Ознакомить с правилами лицензирования и сертификации в области защиты информации, международным законодательством в области защиты информации;
- Привить знания о компьютерных преступлениях и построении систем организационной защиты объектов информатизации.

Требования к результатам освоения дисциплины:

Компетенции, формируемые в результате освоения дисциплины

- ОК-1 — способностью осознавать необходимость соблюдения Конституции Российской Федерации, прав и обязанностей гражданина своей страны, гражданского долга и проявления патриотизма.
- ПК-3 — способностью использовать нормативные правовые документы в своей профессиональной деятельности.

В результате освоения дисциплины студент должен:

знать:

- основы российской правовой системы и законодательства, организации судебных и иных правоприменительных и правоохранительных органов, правовые и нравственно-эстетические нормы в сфере профессиональной деятельности;
- права и свободы человека и гражданина, уметь их реализовать в различных сферах жизнедеятельности;
- содержание основных понятий по правовому обеспечению информационной безопасности;
- правовые способы защиты государственной тайны, конфиденциальной информации и интеллектуальной собственности;
- понятие и виды защищаемой информации, особенности государственной тайны как вида защищаемой информации;
- основы правового регулирования взаимоотношений администрации и персонала в области защиты информации;
- правила лицензирования и сертификации в области защиты информации;
- виды и признаки компьютерных преступлений, особенности основных следственных действий при расследовании указанных преступлений;

уметь:

- использовать нормативные правовые документы, относящиеся к будущей профессиональной деятельности;
- предпринимать необходимые меры к восстановлению нарушенных прав.
- использовать нормативные правовые акты, юридические документы в своей профессиональной деятельности;
- понимать смысл нормативных правовых актов, сопоставлять с другими актами;
- анализировать и интерпретировать нормы права применительно к конкретным ситуациям;
- анализировать и систематизировать разнообразную правовую информацию для достижения целей профессиональной деятельности;
- подготавливать и оформлять документы для регистрации прав на объекты интеллектуальной собственности;
- внедрять и коммерциализировать результаты исследований и разработок в научно-технической сфере, поддерживать меры по обеспечению информационной безопасности в организации и защите прав на объекты интеллектуальной собственности;
- применять современные информационные технологии для поиска и обработки правовых статистических данных, иной правовой информации

владеть:

- навыками общения с использованием специальной лексики и терминологии, позволяющих уяснить многогранную роль права в жизни общества;
- основными методами, способами и средствами получения правовой

информации, в том числе посредством использования нормативно-правовой базы и глобальных компьютерных сетей;
- навыками работы с правовыми актами;
- навыками анализа различных правовых явлений, юридических фактов, правовых норм и правовых отношений, являющихся объектами профессиональной деятельности.
- навыками публичной речи, аргументации, ведения дискуссии.

Содержание дисциплины:

История и теория права и государства.Конституционное право.Основы гражданского права.Основы трудового права.Основы административного права.Основы экологического права.Основы семейного права.

Основы уголовного права.Правоохранительные органы.Правовые основы защиты государственной тайны.Особенности правового регулирования будущей профессиональной деятельности. Информация как объект правового регулирования. Информация как объект юридической защиты. Виды защищаемой информации. Система защиты государственной тайны. Правовой режим защиты государственной тайны. Государственная система правового обеспечения информационной безопасности Законодательство РФ в области информационной безопасности. Основное содержание законов и подзаконных актов по вопросам информационной безопасности. Правовой режим защиты государственной тайны. Подзаконные акты и нормы в области защиты государственной тайны. Правовые режимы защиты конфиденциальной информации. Правовая защита компьютерной информации. Правовые аспекты применения электронной цифровой подписи и защиты информации от технической разведки. Лицензирование и сертификация в информационной сфере. Система сертификации средств защиты информации. Аттестация объектов обработки конфиденциальной информации. Защита интеллектуальной собственности. Правовые аспекты применения электронной цифровой подписи и защиты информации от технической разведки. Основные положения законодательства РФ в области авторского права. Компьютерные правонарушения. Правовая охрана программ для ЭВМ и баз данных. Система лицензирования деятельности организаций по оказанию услуг в области ИБ Правовое регулирование оперативно-розыскных мероприятий (ОРМ) в оперативно-розыскной (ОРД) и частной детективной и охранной деятельности (ЧДОД). Международное законодательство в области защиты информации. Организация защиты информации при осуществлении международного сотрудничества. Защита прав личности в информационной сфере.

Аннотация дисциплины С1.Б.5
«Экономические основы обеспечения компьютерной безопасности»

ТРУДОЕМКОСТЬ ЗЕТ 3 (108 ЧАСОВ)

Цель дисциплины:

Целью изучения учебной дисциплины «Экономика защиты информации» состоит в том, чтобы дать студентам базовые теоретические знания и некоторые практические навыки по экономическому обоснованию затрат и оценкой эффективности создания и эксплуатации технических, организационных и программно-аппаратных средств системы защиты объектов информатизации.

Задачи дисциплины:

- Получение знаний о производственно-хозяйственной деятельности предприятия, как источнике и потребителе информации, которую нужно защищать.
- Получение системы знаний об основных экономических проблемах защиты информации, заключающихся в определении экономического ущерба, нанесенного информации.
- Приобретение навыков в оценке рисков защиты информации и факторов при, определяющих величину ущерба от её потери, при недостаточной надежности её защиты.
- Формирование основных теоретических и практических знаний о подходах к определению экономического ущерба, нанесенного информации, и затрат на её защиту.
- Изучение методов и формирование теоретических знаний и практических навыков оценки и обоснования затрат на создание и функционирование систем защиты информации.
- Формирование специальных теоретических знаний о видах и функциях страхования как способа экономической защиты информации.
- Приобретение теоретических и практических навыков в формирование бюджета службы защиты информации.
- Формирование знаний и практических навыков в выборе методов сопоставительного анализа и оценки инвестиций в комплексные системы защиты, в определении экономической эффективности защиты информации объекта информатизации.

Требования к результатам освоения дисциплины:

Компетенции, формируемые в результате освоения дисциплины

- ОК-4 — способностью понимать и анализировать политические события, мировоззренческие, экономические и социально значимые проблемы и процессы, применять основные положения и методы социальных, гуманитарных и экономических наук при решении социальных и профессиональных задач.
- ПК-13 — способностью к проведению предварительного технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности.
- ПК-32 — способностью организовать мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического

обслуживания средств защиты информации.

- ПК-4 — способностью формировать комплекс мер по информационной безопасности с учётом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности.

В результате освоения дисциплины студент должен:

знать:

- производственно-хозяйственную деятельность предприятия, как источнике и потребителе информации, которую нужно защищать;
- факторы, определяющих величину ущерба от её потери при недостаточной надежности её защиты;
- методы оценки затрат на создание и функционирование систем защиты информации;
- методы оценки инвестиций в систему защиты, видах и функциях страхования защиты информации.

уметь:

- анализировать состояние экономической безопасности организации и правильно определять роль защиты информации в её обеспечении;
- определять расчётным и экспертным путем стоимостные оценки ущерба, наносимого владельцу информации;
- выбирать методы сопоставительного анализа эффективности инвестиционных проектов в защиту информации, анализировать и классифицировать риски, возникающие при защите информации;

определять объекты системы защиты информации, подлежащие первоочередному страхованию и учитывать их в разработке договоров страхования

владеть:

методами определения экономической эффективности инвестиций в комплексные системы защитыинформации.

Содержание дисциплины:

• Введение. Ресурсы предприятия и служб защиты информации. Оценка затрат на создание средств защиты информации. Эффективнсть капиталовложений в создание средств ЗИ. Оценка экономической и информационной безопасности. Страхование рисков

Аннотация программы учебной дисциплины

С1.Б.6 «Управленческая деятельность по обеспечению компьютерной безопасности». *ТРУДОЕМКОСТЬ ЗЕТ 4 (144 ЧАСОВ)*

Цель дисциплины состоит в обеспечении овладения слушателями знаний и навыков в области корпоративного управления с учётом факторов риска компьютерной безопасности компании, необходимых для успешной профессиональной деятельности.

Задачи дисциплины предполагают:

-овладению системными принципами и методами управления, формированию новой отечественной культуры корпоративного управления с учётом угроз компьютерной безопасности;

-решение конкретных проблем корпоративного управления, формирование умений обстоятельно комментировать и практически разъяснять новые нормативные акты в области корпоративного управления по обеспечению компьютерной безопасности, умению обеспечивать баланс интересов корпоративного сектора;

-формирование профессиональных и научных компетенций, позволяющих обеспечить доверие инвесторов, привлечение долгосрочных капиталовложений, в том числе международных инвестиций в целях обеспечения расширенного воспроизводства.

1. **Требования к результатам освоения дисциплины**

Программа направлена на реализацию следующих компетенций:

ОК- 6, ПК- 20, ПК- 27, ПК- 29

В результате освоения дисциплины студент должен:

знать:

- понятие и признаки корпорации;
- сущность корпоративного управления (в узком и широком смысле);
- субъектов корпоративных отношений и их интересов;
- существующие механизмы корпоративного управления и уровни управления в компаниях;
- институциональную основу корпоративного управления.

Уметь:

- различать интересы субъектов корпоративных отношений в целях обеспечения эффективности управления компанией;
- анализировать институциональную основу корпоративного управления с точки зрения реализации основных принципов корпоративного управления в том числе и с учётом обеспечения компьютерной безопасности

Владеть:

методиками разработки процедур и методов контроля уровня информационной безопасности организации;

способностью использовать основные теории мотивации, лидерства и власти для решения управленческих задач;

различными способами разрешения конфликтных ситуаций;

способностью учитывать аспекты корпоративной социальной ответственности при разработке и реализации стратегии организации в контексте обеспечения необходимого уровня компьютерной безопасности.

Содержание дисциплиныОсновные признаки корпорации. Сущность корпоративного управления (в том числе по обеспечению компьютерной безопасности). Основные субъекты корпоративных отношений. Интересы субъектов корпоративного управления с точки зрения компьютерной безопасности. Уровни управления в компаниях. Основные механизмы корпоративного управления. Институциональная основа корпоративного

управления. Внутрикорпоративные расследования и проверки: методики и процедуры проведения. Борьба с корпоративными мошенничествами и противодействие экономическому шпионажу. Кадровая безопасность компании. Профайлинг: детекция лжи и определение характера собеседника. Визуальная диагностика и профайлинг в обеспечении безопасности. Зарубежный опыт.

Аннотация программы учебной дисциплины С1.В.ОД.1 «Основы национальной безопасности»

ТРУДОЕМКОСТЬ ЗЕТ 3 (108 ЧАСОВ)

Цели и задачи дисциплины

Цель преподавания дисциплины "Основы безопасности в Российской Федерации" - дать будущим инженерам, специализирующимся в области комплексного обеспечения безопасности информационных систем или в области организации и технологии защиты информации, основы знаний о состоянии и способах обеспечения безопасности в Российской Федерации и научить их эффективно использовать эти знания.

В процессе изучения дисциплины "Основы безопасности в Российской Федерации" предполагается решить следующие учебные задачи:

-обеспечить знание студентами основных положений и принципов обеспечения национальной безопасности Российской Федерации и основных ее составляющих;

-обеспечить знание студентами конституционных и правовых основ обеспечения национальной безопасности Российской Федерации;

-обеспечить знание студентами основных угроз национальной безопасности Российской Федерации и путей их парирования (нейтрализации);

-ознакомить студентов со структурой и основными функциями органов, решающих задачи обеспечения национальной безопасности в Российской Федерации

Требования к результатам освоения дисциплины

В результате изучения дисциплины студент должен:

знать:

- основные термины и определения в области национальной безопасности РФ, знать основные виды угроз национальной безопасности и методы их парирования, иметь представление о конституционных и правовых основах обеспечения национальной безопасности РФ;

- основные закономерности исторического процесса, этапы исторического развития России, место и роль России в истории человечества и в современном мире.

уметь:

- оценивать возникающие угрозы, прогнозировать развитие региональных конфликтов и кризисных ситуаций;
- использовать в практической деятельности правовые знания,

анализировать основные правовые акты, давать правовую оценку

информации, используемой в профессиональной деятельности.

владеть:

- навыками применения конституционных и правовых норм обеспечения безопасности;
- основными методами научного познания.

Программа направлена на реализацию следующих компетенций: ОК-1; ОК-5; ПК-6; ПК-31.

Содержание дисциплины

Основные понятия безопасности. Концепция национальной безопасности. Основные виды безопасности РФ. Безопасность в регионе

Аннотация программы учебной дисциплины С1.В.ОД.2 «Социотехнические основы информационной безопасности»

ТРУДОЕМКОСТЬ ЗЕТ 4 (144 ЧАСА)

Цели и задачи дисциплины

Цель изучения дисциплины «Социотехнические основы информационной безопасности» - обеспечить будущими инженерам, базовые знания и умения в области обеспечения информационной безопасности социотехнических систем в условиях их сетевого противоборства.

Основными задачами дисциплины являются:

1. Системное знакомство с с социотехническими системами и сетями в контексте обеспечения их устойчивого функционирования.
2. Освоение основ обеспечения безопасности социотехнических систем, функционирующих в условиях сетевого конфликта, включая оценку и регулирование информационных рисков.
3. Знакомство с основами обеспечения информационной безопасности РФ, как социотехнической системы с сетевой организацией, включая отечественную систему подготовки специалистов в области защиты информации.

Требования к результатам освоения дисциплины

В результате изучения дисциплины студент должен:

знать

- содержание и взаимосвязь основных принципов, законов, понятий и категорий гуманитарных социальных и экономических наук в приложении к социотехническим системам;
- сущность организации социотехнических систем и сетей, общесистемные закономерности их функционирования, структурно-функциональное их многообразие;
- содержание Доктрины информационной безопасности РФ и фереральных государственных образовательных стандартов в области защиты информации;

уметь

- использовать принципы, законы и методы гуманитарных, социальных и экономических наук для решения профессиональных задач в области

защиты информации;

- находить метрики и классифицировать социотехнические сети по их структурно-функциональным особенностям, а также – угрозы их безопасности;
- классифицировать социотехнические конфликты, стратегии и тактики их разрешения, прежде всего, в информационном пространстве;

владеть

- понятийным аппаратом в области обеспечения информационной безопасности социотехнических систем, включая определения терминов «конфликт», «угроза», «безопасность», «риск», «ущерб», «информация», «противоборство», «противодействие», «стратегия», «тактика» и т.п.;
- навыками вычисления сетевых метрик и простейшей оценки информационных ущербов и рисков;
- простейшими навыками управления рисками и противодействия угрозам в условиях информационного противоборства социотехнических систем.

Программа направлена на реализацию следующих компетенций:
ОК-5; ОК-9; ПК-5.

Содержание дисциплины

Понятия множества и системы, их математическое описание. Понятие социотехническая система. Общесистемные закономерности в информационном аспекте функционирования социотехнических систем. Сетевая организация современных социотехнических систем. Топологическое определение сетей и их метрики. Структурно-функциональное многообразие современных сетей и метрики их взвешивания.

Понятия конфликта, угрозы и безопасности социотехнических систем и сетей. Понятия информации и безопасности информации. Операции, нарушающие защищенность информации. Понятия ущерба и риска. Классификация сетевых конфликтов в контексте обеспечения информационной безопасности. Стратегии и тактики противоборства в социотехнических сетях и системах. Сетевые войны и управление информационными рисками.

Доктрина обеспечения информационной безопасности РФ, как социотехнической системы с сетевой организацией. Информационное пространство РФ и угрозы нарушения его безопасности в условиях современного противоборства социотехнических систем. Роль кадрового обеспечения в защите информации и отечественная система подготовки кадров в области информационной безопасности. Содержание специальностей подготовки специалистов по защите информации.

Аннотация программы учебной дисциплины С1.В.ДВ.1.1
«Информационно-психологическая безопасность»
ТРУДОЕМКОСТЬ ЗЕТ 3 (108 ЧАСОВ)

- **Цели и задачи дисциплины**

Цели:

– формирование представлений о психике, личности, психологических механизмах информационно-психологического влияния и способах безопасного развития личности;

– удовлетворение познавательных интересов студентов в сфере знаний о человеке вообще и о себе (своих возможностях, достоинствах и недостатках), в частности;

– развитие представлений, способствующих становлению позитивного эмоционально-ценностного отношения к образованию, саморазвитию и самореализации в профессиональной деятельности;

– развитие умений анализировать информационно-психологические факторы, ставить цели и проектировать процесс безопасного развития.

Задачи:

- изучение студентами содержания проблемы информационно-психологической безопасности;
- изучение студентами основ коммуникативного воздействия на психику человека;
- изучение студентами классификации информационно-психологического оружия;
- освоение студентами способов применения информационно-психологического оружия.

Требования к результатам освоения дисциплины

В результате изучения дисциплины студент должен:

знать:

– характеристики психики, личности, основные психологические механизмы информационно-психологического влияния;

– способы и механизмы безопасного развития личности;

– научные основы, цели, принципы, методы и технологии управленческой деятельности;

– способы сотрудничества, групповой работы.

уметь:

– использовать психологические знания для решения практических задач самопознания, безопасного развития, работы в коллективе;

– работать в коллективе, принимать управленческие решения и оценивать их эффективность;

– анализировать собственные возможности, ставить задачи и проектировать процесс саморазвития, включая развитие достоинств и устранение недостатков;

владеть:

- навыками распознавания технологий информационно-психологического воздействия на психику человека и массы людей, а также навыками формирования моделей воздействия и противодействия в информационно-психологической сфере;

- навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности.

Программа направлена на реализацию следующих компетенций: ОК-3; ОК-5; ОК-9. .

Содержание дисциплины

Информационное оружие и информационные войны
Воздействие информации на личность и массы
Способы и приемы информационно-управляющих воздействий

Аннотация рабочей программы дисциплины
С1.В.ДВ.1.2 «История защиты информации»

ТРУДОЕМКОСТЬ ЗЕТ 3 (108 ЧАСОВ)

Дисциплина нацелена на формирование общекультурных компетенций, таких как способность понимать и анализировать политические события, мировоззренческие, экономические и социально значимые проблемы и процессы, применять основные положения и методы социальных, гуманитарных и экономических наук при решении социальных и профессиональных задач; способность осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства ; способность к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления и профессиональных компетенций, таких как способность понимать сущность и значение информации в развитии современного общества, применять достижения информатики и вычислительной техники, перерабатывать большие объемы информации проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах ; способность определять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия

Компетенции, приобретаемые студентами в процессе изучения дисциплины: ОК-9, ПК-4, ПК-5

Цель преподавания данной дисциплины заключается в приобретении знаний и умений по информационной безопасности и защите информации.

Задачи дисциплины раскрыть исторические основы становления и развития системы защиты информации, особенности и тенденции развития организационных структур, способов и средств разведки и защиты информации в различные периоды российского государства.

Специалист должен:

знать:

- историю ведения разведки Россией и против России; анализ исторических этапов становления служб и методов защиты информации в России; принципы развития системы защиты информации в России; принципы современных систем защиты информации в России.

уметь

- использовать в своей деятельности системный подход; применять метод научной аналогии, а также использовать знание исторического опыта оценки угроз безопасности информации и методов противодействия различным угрозам;

владеть

- эволюционным пониманием развития подходов к развитию системы защиты информации.

Содержание дисциплины

Основные этапы развития разведки; основные этапы становления разведки и контрразведки в России; основные этапы развития разведки и контрразведки в СССР и РФ; этапы развития технических средств разведки; этапы развития космической разведки; этапы развития воздушной разведки; этапы развития технических средств наземной разведки; исторический обзор развития криптографических методов защиты информации; этапы развития структуры системы защиты информации в России: защита патентной информации, защита интеллектуальной собственности, государственная система защиты информации

АННОТАЦИЯ
рабочей программы дисциплины «Алгебра и геометрия»

Цели и задачи дисциплины

Дисциплина «Алгебра и геометрия» реализует требования федерального государственного образовательного стандарта высшего профессионального образования по направлению подготовки 10.05.03 «Информационная безопасность автоматизированных систем».

Целью дисциплины является обеспечение фундаментальной подготовки в одной из важнейших областей современной математики; формирование навыков решения геометрических задач в различных системах координат; ознакомление с основами классической и современной алгебры; обучение основным алгебраическим методам решения задач, возникающих в других математических дисциплинах и в практике; ознакомление с историей развития алгебры и геометрии, с вкладом российских ученых в развитие современной алгебраической науки.

Задачами дисциплины являются:

– начальная общематематическая подготовка студентов путем изучения достаточно простых математических конструкций, которые в последующих математических дисциплинах будут обобщаться,

– обучение простейшей алгебраической структуре - векторной алгебре и ее приложениям, формирование навыков использования координатного метода,

– формирование навыков применения алгебраических методов для упрощения уравнений линий и поверхностей второго порядка,

– ознакомление с различными алгебраическими структурами (кольцами, полями, векторными пространствами) и их приложениями в решении различных практических задач,

– освоение методов линейной алгебры широко используемых в различных дисциплинах, в том числе профессиональных,

– воспитание у студентов математической и технической культуры, которая предполагает четкое осознание необходимости и важности математической подготовки для специалиста в области информационной безопасности.

Компетенции, формируемые в результате освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– способность к логическому мышлению, обобщению, анализу, критическому осмыслению информации, систематизации, прогнозированию, постановке исследовательских задач и выбору путей их решения на основании принципов научного познания (ОК-9);

– способность выявлять естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности, и применять соответствующий физико-математический аппарат для их формализации, анализа и выработки решения (ПК-1);

– способность применять математический аппарат, в том числе с использованием вычислительной техники, для решения профессиональных задач (ПК-2);

Требования к уровню освоения содержания дисциплины

В результате изучения дисциплины студент должен:

Знать:

– возможности координатного метода для исследования различных геометрических объектов;

– основные понятия и задачи векторной алгебры и аналитической геометрии;

– основные виды уравнений простейших геометрических объектов;

– основные свойства алгебраических структур;

– основы линейной алгебры над произвольными полями;

– векторные пространства над полями и их свойства.

Уметь:

– строить и изучать математические модели конкретных явлений и процессов для решения расчетных и исследовательских задач;

– определять возможности применения теоретических положений и методов математических дисциплин для постановки и решения конкретных прикладных задач;
– исследовать простейшие геометрические объекты по их уравнениям в различных системах координат;
– оперировать с числовыми и конечными полями, многочленами, матрицами;
– решать основные задачи линейной алгебры, в частности системы линейных уравнений над полями.

Владеть:

– навыками использования методов аналитической геометрии и векторной алгебры в смежных дисциплинах и физике;
– методами линейной алгебры.

Краткое содержание дисциплины

Общая трудоемкость дисциплины составляет 11 зачетных единиц (396 часов).

Продолжительность изучения дисциплины составляет 3 семестра.

В ходе изучения дисциплины «Алгебра и геометрия» студенты усваивают знания по следующей тематике.

Векторная алгебра; аналитическая геометрия на плоскости и в пространстве; матрицы и операции над ними; определители матриц; обратимые матрицы; ранг матрицы; системы линейных уравнений; основные алгебраические структуры: полугруппы, группы, кольца, поля и их свойства; поле комплексных чисел; делимость и деление с остатком в кольце целых чисел; основная теорема арифметики; кольца и поля вычетов; уравнения в кольце вычетов и сравнения; кольцо многочленов; каноническое разложение многочлена; использование многочленов для построения конечных колец и полей; основы теории групп и теории групп подстановок; разложение группы в смежные классы; нормальные делители группы; векторные пространства и их линейные преобразования; евклидовы и унитарные пространства, линейные преобразования евклидовых и унитарных пространств; квадратичные формы.

Аннотация рабочей программы дисциплины
С2.Б2. Математический анализ

Трудоемкость 11 ЗЕТ (396 часа)

Цель дисциплины – ознакомить обучаемых с основными понятиями и методами математического анализа, создать теоретическую и практическую базу подготовки специалистов к деятельности, связанной с проектированием, разработкой и применением электронной аппаратуры для обеспечения безопасности автоматизированных систем.

Задача дисциплины – привить обучаемым навыки использования рассматриваемого математического аппарата в профессиональной деятельности и воспитать у обучаемых высокую культуру мышления.

Компетенции, формируемые в результате освоения дисциплины:

ОК-10; ПК-1, ПК-2.

В результате освоения дисциплины студент должен

знать

– основные положения теории пределов функций, теории рядов;

– основные теоремы дифференциального и интегрального исчисления функций одного и нескольких переменных;

уметь

– строить и изучать математические модели конкретных явлений и процессов для решения расчетных и исследовательских задач;

– определять возможности применения теоретичесикх положений и методов математических дисциплин для постановки и решения конкретных прикладных задач;

– решать основные задачи на вычисление пределов функций, дифференцирование и интегрирование, на разложение функций в ряды;

– пользоваться расчетными формулами, таблицами, компьютерными программами при решении математических задач;

владеть

– навыками использования стандартных методов и моделей математического анализа и их применения к решению прикладных задач;

– навыками пользования библиотеками прикладных программ для решения прикладных математических задач.

Краткое содержание дисциплины:

Действительные числа. Понятие функции. Теория пределов. Дифференциальное исчисление функций одного и нескольких переменных. Интегральное исчисление функций одного и нескольких переменных. Криволинейные интегралы. Метрические пространства. Числовые и функциональные ряды. Элементы теории функций комплексного переменного. Элементы теории обыкновенных дифференциальных уравнений. Ряды Фурье. Преобразования Фурье и Лапласа.

Аннотация рабочей программы дисциплины
С2.Б.3. Дискретная математика

Трудоемкость 6 ЗЕТ (216 часа)

Целью дисциплины является ознакомление обучающихся с основами общей комбинаторики, теории графов, теории кодирования и теории автоматов.

Задачами дисциплины являются:

воспитание у студентов математической и технической культуры,

четкое осознание необходимости и важности математической подготовки для специалиста технического профиля,

ознакомление с основными объектами и методами дискретной математики, а также их приложениями для решения различных задач, требующих применения вычислительных средств,

развитие навыков обращения с дискретными конструкциями и умения строить математические модели объектов и процессов, с которыми имеет дело бакалавр в ходе своей профессиональной деятельности.

Компетенции, формируемые в результате освоения дисциплины:

способность к логическому мышлению, обобщению, анализу, критическому осмыслению информации, систематизации, прогнозированию, постановке исследовательских задач и выбору путей их решения на основании принципов научного познания (ОК-9);

способность выявлять естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности, и применять соответствующий физико-математический аппарат для их формализации, анализа и выработки решения (ПК-1);

способность применять математический аппарат, в том числе с использованием вычислительной техники, для решения профессиональных задач (ПК-2);

В результате освоения дисциплины студент должен

Знать

основы комбинаторного анализа;

метод включения-исключения; производящие функции;

основные понятия теории автоматов;

основные понятия и алгоритмы теории графов;

основные дискретные структуры: конечные автоматы, графы, комбинаторные структуры;

методы перечисления для основных дискретных структур;

основные методы оптимального кодирования источников информации и помехоустойчивого кодирования каналов связи;

Уметь

- применять стандартные методы дискретной математики и теории автоматов для решения профессиональных задач;
- решать задачи периодичности и эквивалентности для конечных автоматов;
- применять аппарат производящих функций и рекуррентных соотношений для решения перечислительных задач;
- решать оптимизационные задачи на графах;

Владеть

навыками построения дискретных моделей при решении профессиональных задач;

навыками применения языка и средств дискретной математики;

навыками решения комбинаторных и теоретико-графовых задач;

навыками применения математического аппарата для решения прикладных теоретико-информационных задач.

Краткое содержание дисциплины:

Основы комбинаторики. Бинарные отношения. Метод включения-исключения. Метод производящих функций. Основные понятия теории графов. Эйлеровы и гамильтоновы графы. Деревья. Метрические характеристики графа. Укладки и раскраски. Элементы теории кодирования. Линейные коды. Коды Хэмминга и циклический. Основные понятия теории автоматов. Линей-

ные автоматы над конечным полем. Эксперименты по распознаванию состояний автоматов. Эксперименты по распознаванию автоматов.

Аннотация рабочей программы дисциплины
С2.Б4. Теория вероятностей и математическая статистика

Трудоемкость 10 ЗЕТ (360 часа)

Цель дисциплины – ознакомить обучаемых с основными понятиями и методами теории вероятностей, теории случайных процессов и математической статистики, обеспечить теоретическую и практическую подготовку специалистов к деятельности, связанных с проектированием, созданием, исследованием и эксплуатацией систем обеспечения информационной безопасности телекоммуникационных систем в условиях существования угроз в информационной сфере.

Задача дисциплины – привить обучаемым навыки использования рассматриваемого математического аппарата в профессиональной деятельности и воспитать у обучаемых высокую культуру мышления.

Компетенции, формируемые в результате освоения дисциплины:

ПК-1 ПК-2

В результате освоения дисциплины студент должен

знать

– основные понятия и методы теории вероятностей, теории случайных процессов и математической статистики;

уметь

– строить и изучать математические модели конкретных явлений и процессов для решения расчетных и исследовательских задач;

– определять возможности применения теоретичесикх положений и методов математических дисциплин для постановки и решения конкретных прикладных задач;

– применять стандартные методы и модели к решению типовых теоретико-вероятностных и статистических задач;

– пользоваться расчетными формулами, таблицами, компьютерными программами при решении математических задач;

владеть

– навыками использования стандартных теоретико-вероятностных и статистических методов при решении прикладных задач;

– навыками пользования библиотеками прикладных программ для решения прикладных математических задач;

Краткое содержание дисциплины:

Алгебра событий. Вероятностное пространство. Основные теоремы теории вероятностей. Одномерные случайные величины. Числовые характеристики случайных величин. Основные распределения случайных величин. Многомерные случайные величины. Числовые характеристики многомерных случайных величин. Функции случайных величин. Предельные теоремы. Случайные процессы. Дискретные цепи Маркова. Марковские процессы с не-

прерывным временем. Выборочный метод. Оценки параметров распределения. Статистическая проверка гипотез. Метод статистических испытаний. Обработка экспериментальных данных. Непараметрические методы статистики.

Аннотация рабочей программы дисциплины С2.Б.5. Математическая логика и теория алгоритмов

Трудоемкость 4 ЗЕТ (144 часа)

Целью освоения дисциплины является ознакомление студентов с основами математической логики и теории алгоритмов, методами оценки сложности алгоритмов и построения эффективных алгоритмов, а также обеспечение фундаментальной подготовки в одной из важнейших областей современной математики.

Задачами дисциплины являются:

– формирование научного мировоззрения, понимания широты и универсальности методов математической логики, умения применять эти методы в решении прикладных задач,

– развитие творческого мышления, математической грамотности, способности критически анализировать собственные рассуждения и самостоятельно их корректировать,

– воспитание математической культуры, которая предполагает четкое осознание необходимости и важности математической подготовки для специалиста в области компьютерной безопасности,

– ознакомление с основными объектами математической логики, а также их приложениями для решения различных задач, требующих применения вычислительных средств,

– выработка навыков обращения с дискретными конструкциями и умения строить математические модели объектов и процессов, с которыми имеет дело специалист в ходе своей профессиональной деятельности.

Компетенции, формируемые в результате освоения дисциплины:

ОК-9, ПК-1, ПК-2.

В результате освоения дисциплины студент должен

Знать

– основные понятия математической логики и теории алгоритмов;

– язык и средства современной математической логики,

– представления булевых функций и способы минимизации формул;

– типовые свойства и способы задания функций многозначной логики.

– различные подходы к определению алгоритма и доказательства алгоритмической неразрешимости отдельных массовых задач,

– подходы к оценкам сложности алгоритмов,

– методы построения эффективных алгоритмов,

– возможности применения общих логических принципов в математике и профессиональной деятельности,

Уметь

- находить и исследовать свойства представлений булевых и многозначных функций формулами в различных базисах;
- оценивать сложность алгоритмов и вычислений;
- классифицировать алгоритмы по классам сложности.
- применять методы математической логики и теории алгоритмов к решению задач математической кибернетики,

Владеть

- навыками использования языка современной символической логики;
- навыками применения методов и фактов теории алгоритмов, относящимися к решению переборных задач;
- навыками упрощения формул алгебры высказываний и алгебры предикатов;
- навыками составления программ на машинах Тьюринга.

Краткое содержание дисциплины:

Алгебра высказываний и алгебра предикатов. Булевы функции и их обобщение. Исчисление высказываний. Исчисление предикатов. Метод резолюций. Элементы теории алгоритмов. Алгоритмическая разрешимость и неразрешимость. Сложность алгоритмов и вычислений. Методы построения эффективных алгоритмов. Сложностная классификация переборных задач. Теория алгоритмов и задачи использования ЭВМ.

Аннотация программы учебной дисциплины С2.Б.6 «Теория информации»

Трудоемкость 3 ЗЕТ (108 часов)

Цели и задачи дисциплины

Целью дисциплины является изучение основных положения теории информации, элементов обобщённой спектральной теории сигналов, вопросов сжатия сообщений и помехоустойчивого кодирования.

Задачами дисциплины являются:

- ознакомление студентов с местом теории информации в ряду естественнонаучных и прикладных дисциплин,
- ознакомление со способами представления информации, методами получения, накопления и обработки информации в вычислительных системах.
- выработка практических навыков применения методов теории информации в исследовательской и инженерной деятельности;

Требования к уровню освоения содержания дисциплины

В результате освоения дисциплины

студент должен знать:

- закономерности протекания информационных процессов в искусственных системах и методы анализа этих процессов;
- основные понятия теории информации и кодирования:

энтропия, взаимная информация, источники сообщений, каналы связи, коды;

- методы сжатия данных;
- методы контроля и коррекции ошибок;
- математические модели сигналов и процессов обработки информации.

уметь:

- производить анализ и выбор систем кодирования информации по заданным условиям избыточности и помехоустойчивости;
- применять стандартные методы и модели к решению типовых теоретико-вероятностных и статистических задач;
- проектировать на функционально-логическом уровне кодирующие, декодирующие, контрольные и другие узлы цифровой аппаратуры.

владеть:

- методами сжатия данных;
- методами контроля и коррекции ошибок;
- навыками использования стандартных методов и моделей математического анализа и их применения к решению прикладных задач;
- навыками проектирования кодирующих, декодирующих, контрольных и других узлов цифровой аппаратуры.

Программа направлена на реализацию следующих компетенций: ОК-9, ОК-10.

Содержание дисциплины, основные разделы

Введение в теорию информации. Основные понятия теории информации. Сигналы. Виды модуляции. Спектры сигналов. Распределение энергии в спектре. Общие принципы преобразования сигналов. Измерение информации. Энтропия сообщений. Марковские и эргодические источники. Сжатие сообщений. Арифметическое кодирование. Статистическое моделирование источников информации. Сжатие информации с потерями. Фрактальное сжатие изображений. Контроль и диагностика ошибок в информационных системах. Принципы помехоустойчивого кодирования. Линейные коды. Циклические коды. Обзор проблем помехоустойчивого кодирования. Информационные характеристики дискретных каналов связи.

Аннотация программы учебной дисциплины С2.Б.7 «Информатика»

Трудоемкость 4 ЗЕТ (144 часа)

- **Цели и задачи дисциплины**

Целью изучения дисциплины «Информатика» является формирование общей информационной культуры студентов, подготовка их к деятельности,

связанной с использованием современных информационных технологий.

Задачи дисциплины:

изучение основных понятий информатики;

изучение свойств и способов записи алгоритмов;

изучение способов представления чисел, символов, графики, аудио- и видеоинформации в персональном компьютере;

ознакомление с логическими основами устройства ЭВМ;

ознакомление с составом и назначением функциональных узлов компьютера;

изучение основ построения операционных систем (ОС) на примере ОС с открытым
кодом;

изучение основ программирования в командных оболочках;

овладение навыками применения сервисных программных средств системного и прикладного назначения;

изучение основ построения компьютерных сетей;

овладение навыками поиска информации в глобальной информационной сети Интернет.

- **Требования к уровню освоения содержания дисциплины**

В результате изучения дисциплины

студент должен **знать:**

основные понятия информатики;

формы и способы представления данных в персональном компьютере;

состав, назначение функциональных компонентов и программного обеспечения персонального компьютера;

классификацию современных компьютерных систем;

типовые структуры и принципы организации компьютерных сетей;

уметь:

применять типовые программные средства сервисного назначения (средства восстановления системы после сбоев, дефрагментации и очистки диска);

пользоваться сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети Интернет;

владеть:

навыками работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов);

навыками обеспечения безопасности информации с помощью типовых программных средств (антивирусов, архиваторов, стандартных сетевых средств обмена информацией).

Программа направлена на реализацию следующих компетенций:

ПК-2, ПК-4, ПК-8, ПК-10, ПК-17.

- **Содержание дисциплины, основные разделы**

Основные понятия информатики. Основы построения ЭВМ. Программное обеспечение ЭВМ. Компьютерные сети.

Аннотация программы дисциплины С2.Б.8 «Физика»

Трудоемкость 10 ЗЕТ (360 часов)

Цели изучения дисциплины

– обеспечение фундаментальной физической подготовки, позволяющей будущим специалистам ориентироваться в научно-технической информации, использовать физические принципы и законы, а также результаты физических открытий в тех областях техники, в которых они будут трудиться;

- ознакомление студентов с современной физической картиной мира, с основными концепциями, моделями, теориями, описывающими поведение объектов в микро-, макро- и мегамире, с состоянием переднего края физической науки;

- приобретение навыков экспериментального исследования физических процессов, освоение методов получения и обработки эмпирической информации;

- изучение теоретических методов анализа физических явлений, расчетных процедур и алгоритмов, наиболее широко применяемых в физике.

.Основные дидактические единицы (разделы)

Физические основы механики: понятие состояния в классической механике, уравнения движения, законы сохранения, основы релятивистской механики, принцип относительности в механике, кинематика и динамика твердого тела, жидкостей и газов; электричество и магнетизм: электростатика и магнитостатика в вакууме и веществе, уравнения Максвелла в интегральной и дифференциальной форме, материальные уравнения, квазистационарные токи, принцип относительности в электродинамике; физика колебаний и волн: гармонический и ангармонический осциллятор, физический смысл спектрального разложения, кинематика волновых процессов, нормальные моды, интерференция и дифракция волн, элементы Фурье-оптики; квантовая физика: корпускулярно-волновой дуализм, принцип неопределенности, квантовые состояния, принцип суперпозиции, квантовые уравнения движения, операторы физических величин, атомная физика, физика ядра и элементарных частиц; статистическая физика и термодинамика: три начала термодинамики, термодинамические функции состояния, фазовые равновесия и фазовые превращения, элементы неравновесной термодинамики, классическая и квантовые статистики, кинетические явления, системы заряженных частиц, конденсированное состояние; физический практикум.

Компетенции, приобретаемые студентом в процессе изучения дисциплины ОК-7, ОК-9, ОК-10, ПК-1, ПК-2, ПК-5.

В результате изучения дисциплины студент должен:

знать:

Основные законы механики; основные законы термодинамики и молекулярной физики; основные законы электричества и магнетизма; основы

теории колебаний и волн, оптики; основы квантовой физики и физики твердого тела; физические явления и эффекты, используемые при обеспечении ИБ АС;

уметь:

вычислять теоретико-информационные характеристики источников сообщений и каналов связи; решать типовые задачи кодирования и декодирования; строить математические модели физических явлений и процессов; решать типовые прикладные физические задачи; анализировать и применять физические явления и эффекты для решения практических задач обеспечения информационной безопасности;

владеть:

навыками применения математического аппарата для решения прикладных теоретико-информационных задач; методами теоретического исследования физических явлений и процессов; навыками проведения физического эксперимента и обработки его результатов.

Аннотация к рабочей программе по дисциплине «Исследование операций и теория игр»

Цели и задачи дисциплины: учебная дисциплина «Исследование операций и теория игр» реализует требования федерального государственного образовательного стандарта высшего профессионального образования по специальности 090303 «Информационная безопасность автоматизированных систем».

Цель дисциплины – ознакомить обучаемых с основными понятиями и методами исследования операций и теории игр.

Задачи дисциплины – привить обучаемым навыки использования рассматриваемого математического аппарата в профессиональной деятельности и воспитать у обучаемых высокую культуру мышления, т.е. строгость, последовательность, непротиворечивость и основательность в суждениях, в том числе и в повседневной жизни.

Учебная дисциплина «Исследование операций и теория игр» является составной частью профессиональной подготовки по специальности 090303 «Информационная безопасность автоматизированных систем».

Требования к уровню усвоения дисциплины.

Процесс изучения дисциплины направлен на формирование следующих компетенций:

профессиональные компетенции: ОК-9, ПК-1, ПК-2.

В результате усвоения дисциплины должен:

Знать:

1. общую постановку задач математичесого программирования, теории игр, имитационного моделирования, сетевого планирования;
2. универсальные приёмы исследования оптимизационных проблем при различной степени неопределённости условий;

Уметь:

1. формировать множество альтернативных решений, ставить цель и

выбрать оценочный критерий оптимальности, сформулировать ограничения на управляемые переменные, связанные со спецификой моделируемой системы;

2. обосновать выбор подходящего математического метода и привести алгоритм решения задачи;

Владеть:

3. навыками построения и анализа моделей типичных операционных задач.

Содержание дисциплины

Математическая модель операции, её компоненты, стратегии игр.

Многокритериальные задачи выбора и принятия решений.

Принятие решений в конфликтных ситуациях. Антагонистические игры.

Бескоалиционные и иерархические игры.

Сетевые задачи.

Теория игр и принятие решений в условиях информационного противоборства.

Статистические методы принятия решений

Аннотация к рабочей программе дисциплины «Теория графов и её приложения»

Трудоемкость 4 ЗЕТ (144 часа)

Цель дисциплины – ознакомить обучаемых с основными понятиями и методами исследования операций и теории игр и их приложениями к анализу и синтезу линейных систем.

Задача дисциплины – привить обучаемым навыки использования рассматриваемого математического аппарата в профессиональной деятельности и воспитать у обучаемых высокую культуру мышления, т.е. строгость, последовательность, непротиворечивость и основательность в суждениях, в том числе и в повседневной жизни.

Требования к результатам освоения дисциплины:

Процесс изучения дисциплины направлен на формирование следующих компетенций: ОК-7, ОК-9, ОК-10, ПК-1, ПК-2, ПК-5, ПК-9, ПК-22.

В результате изучения дисциплины обучаемый должен:

Знать: основные операции над графами: объединение и пересечение графов; универсальные приёмы исследования оптимизационных проблем на графах в

Уметь: строить матрицы смежности, инциденций, связности, достижимости графов, выделять компонеты связности и сильной связности графов; обосновать выбор подходящего математического метода и привести алгоритм решения задачи;

Владеть: навыками построения и анализа моделей типичных прикладных задач с помощью графов.

Содержание дисциплины

Основы теории графов

Виды и способы задания графов. Подграфы и части графа. Операции над графами. Маршруты. Достижимость. Связность. Разложение графа на компоненты связности. Расстояние в графах. Метрические характеристики графов. Степени вершин. Теорема Эйлера о сумме степеней. Циклы в графах. Цикломатическое число. Дерево. Лес. Остовы графов. Наименьший остов. Рёберная и вершинная связность. Упорядоченные и бинарные деревья. Фундаментальные циклы Графы, связанные с группами. Изоморфизм графов. Группа автоморфизмов. Планарные графы. Теорема Понтрягина-Куратовского. Критерий планарности.

Приложения теории графов

Уравнения линейных систем. Основные типы графов линейных систем. Определение взаимосвязи переменных в графах. Расчёт функций линейных систем с помощью графов. Алгоритм анализа линейных систем с помощью графов. Алгоритмы автоматизированного расчёта функций с помощью графов. Расчёт функций сложных линейных систем с помощью графов. Особенности расчёта сложных систем. Расчёт схемных функций посредством свёртывания модели и по частям. Функции чувствительности. Расчёт функций чувствительности линейных систем с помощью графов. Основы синтеза линейных систем с помощью графов. Переход от передаточной функции к графу и от графа к линейной системе. Синтез линейных аналоговых систем с помощью графов. Синтез систем по заданным передаточным функциям и с использованием функций чувствительности. Синтез линейных цифровых систем с помощью графов. Обобщённая схема размещения и компоненты случайных графов. Эволюция случайных графов. Докритические и критические графы. Случайные графы с независимыми рёбрами. Неравновероятные графы. Системы случайных линейных уравнений в GF(2). Случайные подстановки. Сети Петри и графовое представление марковских и полумарковских процессов. Топологические модели социальных информационных сетей: модели влияния, управления и противоборства.

Аннотация программы учебной дисциплины С2.В.ОД.1 «Физические основы защиты информации»

Трудоемкость 4 ЗЕТ (144 часа)

Цель дисциплины: дать будущим инженерам, специализирующимся в области информационной **безопасности** распределенных информационных систем, основы знаний о физических каналах утечки защищаемой информации, принципах построения и способах применения технических средств защиты информации в различных физических полях и научить их эффективно использовать эти знания.

Задачи дисциплины:

обеспечить знание студентами основных задач в рамках общей проблемы безопасности информации, решаемых методами и средствами защиты информации от технических разведок;

обеспечить знание студентами физических основ утечки защищаемой информации в различных физических полях ;

обеспечить знание студентами практических навыков применения существующих мер и средств защиты информации от технических разведок.

Требования к результатам освоения дисциплины:

Компетенции, формируемые в результате освоения дисциплины:

ОК-5, ОК-7, ОК-9, ОК-10, ПК-1, ПК-2, ПК-3, ПК-7, ПК-8, ПК-10

В результате освоения дисциплины студент должен:

- знать:

цели, задачи и организация технических разведки;

классификацию технических разведок по различным признакам;

основные характеристики космической, воздушной, морской, наземной и компьютерной разведок;

методические основы защиты информации от радиоэлектронной разведки;

методические основы защиты информации от оптико-электронной разведки;

методические основы защиты информации от акустической разведки;

методические основы защиты информации от компьютерной разведки

уметь:

определять перечень потенциально опасных средств разведки для объекта защиты;

решать типовые задачи оценки возможностей технических разведок;

обосновывать эффективность средств защиты информации

владеть:

методами теоретического исследования технических каналов утечки информации;

навыками проведения расчетов показателей эффективности защиты информации.

Содержание дисциплины:

Раздел 1	Цели, задачи и организация технической разведки
Раздел 2	Характеристика видов технической разведки
Раздел 3	Методические основы защиты информации от радиоэлектронной разведки
Раздел 4	Методические основы защиты информации от оптико-электронной разведки
Раздел 5	Методические основы защиты информации от акустической разведки
Раздел 6	Методические основы комплексной защиты информации
Раздел 7	Методические основы защиты информации от компьютерной разведки

Аннотация программы учебной дисциплины С2.В.ОД.2
«Математические основы риск-анализа»
Трудоемкость 4 ЗЕТ (144 часа)

Цель изучения дисциплины «Математические основы риск-анализа» - дать студентам общие сведения и представления о методах и средствах исследования систем различного характера с помощью аппарата риск-анализа.

Основными задачами дисциплины являются:

ознакомить студентов с основными отечественными и зарубежными стандартами и методами анализа рисков;

ознакомить студентов с математическими методами обработки экспериментальных данных;

дать студентам основы принципов использования качественных и количественных методов исследования риска.

Требования к результатам освоения дисциплины

В результате изучения дисциплины студент должен:

знать основные отечественные и зарубежные стандарты в области защиты информации, математические методы обработки экспериментальных данных, методы анализа рисков;

уметь использовать математические методы и модели для решения прикладных задач;

владеть методами количественного риск-анализа процессов обработки, поиска и передачи информации.

Программа направлена на реализацию следующих компетенций:

ОК-5, ОК-7, ОК-9, ОК-10, ПК-2, ПК-5, ПК-8, ПК-24.

Содержание дисциплины

Место риск-анализа в системе знаний по обеспечению безопасности систем и процессов. Понятийный аппарат и терминологическая база дисциплины. Оценка рисков и международные страдарты ISO/IEC 17799:2000(E), ISO/IEC TR 13335-2, NIST800-30, Cobit, SCORE, SYS Trust. Концепции управления рисками OCTAVE, CRAMM, MITRE. Инструментарий управления информационными рисками. Методы анализа рисков на основе экспертных оценок и аппарата теории нечетких множеств. Методы управления информационными рисками в инновационной деятельности. Меры риска и защищенности систем на основе вероятностных параметров и характеристик ущерба. Функции чувствительности и динамическое моделирование рисков. Оценка рисков сложных систем на основе параметров рисков их компонентов. Аналитическая оценка рисков при нормальном и логнормальном распределениях плотности вероятности наступления ущерба (ПВНУ). Аналитическая оценка рисков при гамма и бета-распределениях ПВНУ.

Аналитическая оценка рисков при экспоненциальном, Вейбулла и Эрланга распределениях ПВНУ. Аналитические риск-модели при биномиальном, Паскаля и мультинормальном распределениях вероятности наступления ущерба (ВНУ). Аналитические риск-модели при геометрическом и гипергеометрическом распределениях ВНУ. Аналитические риск-модели при пуассоновском распределении ВНУ и распределениях типа А и В. Нерегулярные распределения ущерба и динамика рисков. Синтез систем с заданным риском. Прогнозирование эффективности систем на основе анализа рисков ущербности и шансов полезности.

Аннотация программы учебной дисциплины С2.В.ДВ.1.1
«Математические основы управления рисками»

Трудоемкость 4 ЗЕТ (144 часа)

Целью изучения дисциплины является изучение основных этапов процесса управления рисками информационной безопасности как одной из основных составляющих системы менеджмента информационной безопасности; знакомство с методами принятия решений (экспертных оценок, многокритериального принятия решений при определенности и при неопределенности, обусловленной как случайными воздействиями внешней среды, так и действиями злоумышленника) как математической основой выбора оптимальных защитных мероприятий, направленных на снижение риска информационной безопасности.

Задачи дисциплины:

- изучение основных понятий и методов управления рисками информационной безопасности;
- знакомство с менеджментом риска информационной безопасности, включая основные этапы: установление контекста, оценку, обработку, принятие и коммуникацию риска, а также мониторинг и переоценку риска информационной безопасности;
- знакомство с современными стандартами в области управления информационными рисками;
- знакомство с существующими инструментальными средствами для управления рисками;
- изучение методов экспертных оценок, как основного инструмента принятия решений при управлении рисками информационной безопасности в условиях недостаточности объективной информации;
- изучение методов многокритериального принятия решений при определенности (аксиоматических методов многокритериальной оценки альтернатив, метода аналитической иерархии, метода порогов несравнимости);
- изучение статистических моделей и методов принятия решений при неопределенности, обусловленной случайными воздействиями внешней среды;

- изучение статистических моделей и методов принятия решений при неопределенности, обусловленной действиями злоумышленника;

- знакомство с методами оптимизации.

Требования к уровню освоения содержания дисциплины

В результате изучения дисциплины студент

должен **знать:**

- основные понятия и методы управления рисками информационной безопасности;
- основные этапы менеджмента риска информационной безопасности;
- современные стандарты в области управления информационными рисками;
- основные понятия и обобщенную классификацию задач принятия решений при управлении рисками информационной безопасности;
- формальное описание моделей принятия решений при управлении рисками информационной безопасности;
- методы экспертных оценок и варианты их использования при управлении рисками информационной безопасности;
- детерминированные модели и методы принятия решений при управлении рисками информационной безопасности;
- статистические модели и методы принятия решений в условиях неопределенности, обусловленной как случайными воздействиями внешней среды, так и действиями злоумышленника;
- разновидности оптимизационных моделей и варианты их использования при управлении рисками информационной безопасности.

уметь:

- организовать систему менеджмента риска информационной безопасности в соответствии со стандартом ГОСТ Р ИСО/МЭК 27001-2006;
- разрабатывать планы обработки рисков информационной безопасности;
- организовать процедуру экспертного оценивания и осуществить обработку экспертной информации;
- формировать множество альтернатив и критерии оптимальности для задач принятия решений при управлении рисками информационной безопасности;
- решать детерминированную многокритериальную задачу выбора мер контроля и управления, направленных на снижение риска информационной безопасности;
- решать многокритериальную задачу выбора мер контроля и управления в условиях неопределенности, обусловленной как случайными воздействиями внешней среды, так и действиями злоумышленника;
- осуществлять постановку оптимизационной задачи выбора защитных мероприятий, направленных на снижение риска информационной безопасности и выбор метода ее решения.

владеть:

- профессиональной терминологией в области менеджмента рисков информационной безопасности;

- методикой менеджмента риска информационной безопасности в соответствии со стандартом ГОСТ Р ИСО/МЭК 27001-2006;

- методикой проведения экспертного оценивания при решении задачи оценки рисков информационной безопасности и управления ими;

- детерминированными методами принятия решений по управлению рисками информационной безопасности (аксиоматическими методами многокритериальной оценки альтернатив, методом аналитической иерархии, методом порогов несравнимости);

- статистическими методами принятия решений по управлению рисками информационной безопасности в условиях неопределенности, обусловленной как случайными воздействиями внешней среды, так и действиями злоумышленника;

- навыками формирования оптимизационных задач, разработки соответствующих оптимизационных моделей и выбора методов их решения.

Программа направлена на реализацию следующих компетенций: ПК-1, ПК-2, ПК-14, ПК-15, ПСК-7.3

Содержание дисциплины, основные разделы

Менеджмент риска информационной безопасности: основные термины и определения; система менеджмента информационной безопасности; менеджмент риска информационной безопасности; стандарты в области управления информационными рисками; инструментальные средства для управления рисками.

Математические основы принятия решений при управлении рисками: основные понятия и обобщенная классификация задач принятия решений; формальное описание моделей принятия решений; методы экспертных оценок; детерминированные модели и методы принятия решений; статистические модели и методы принятия решений в условиях неопределенности; методы оптимизации.

Аннотация программы дисциплины С2.В2.ДВ.1 «Математические модели информационного противоборства»

Трудоемкость 4 ЗЕТ (144 часа)

Цель и задачи изучаемой дисциплины

Основная цель состоит в основ моделирования информационного противоборства, включая кибертерроризм и экстремизм, основанные на применении насилия в целях изменения общественного сознания и направленные на получение несанкционированного доступа к данным, имеющим определенную ценность и использование их в своих целях.

Основные дидактические единицы (разделы)

Информационная сущность противоборства. Моделирование информационно-управляющих воздействий деструктивного характера.

Моделирование антитеррористической деятельности. Модели возможных операций по локализации информационно-психологических последствий террористических актов и пропаганды терроризма. Системный подход к информационно-аналитическому обеспечению антитеррористической деятельности. Направление создания антитеррористической информационно-аналитической системы.

Компетенции, приобретаемые студентом в процессе изучения дисциплины: ОК-10, ПК-1, ПК-2.

В результате изучения дисциплины студенты должны:

знать:

- способы и приемы террористических и деструктивных воздействий на информационные системы; основы построения антитеррористических информационно-аналитических систем;
- основы построения моделей для защиты от террористических и деструктивных воздействий;
- уязвимые места информационных систем, чаще всего подвергающиеся атакам;

уметь:

- создавать модели информационного противоборства для защиты от деструктивных воздействий;

владеть:

- навыками построения математических моделей эффективных систем информационного противоборства.

Аннотация программы дисциплины
С2.В.ДВ.1 «Математическое моделирование ИОА»

Трудоемкость 4 ЗЕТ (144 часа)

Цели и задачи изучения дисциплины

Основная цель состоит в изучении обобщенных моделей информационных операций и атак (ИОА), реализуемых в отношении социотехнических информационных систем (СТИС).

Задачи изучения дисциплины состоит в возможности на основе освоения теоретических аспектов проблемы строить риск-модели ИОА для различных СТИС.

Основные диалектические единицы (разделы)

Свойства и характеристики ИОА. Оценка уровня опасности атак для СТИС. Информационные операции в социотехнических системах: анализ разновидностей и методология синтеза моделей в приложении к сетевым компьютерным атакам на информационно-телекоммуникационные системы (ИТКС). Модель информационной ИОА на основе деревьев атак Шнайера. Достоинства и недостатки модели деревьев атак Шнайера. Модели ИОА на основе онтологий и формальных языков. Модели ИОА на основе стохастических сетей Петри. Многоагентные технологии моделирования и управления. Требования к моделям ИОА. Управляющие Е-сети как

функциональная основа моделей атак. Имитационное моделирование распределённой атаки типа «отказ в обслуживании». Модели информационно-психологических операций.

Компетенции, приобретаемые студентом в процессе изучения дисциплины ПК-2, ПК-13, ПК-21.

В результате изучения дисциплины студенты должны:

знать:

- разновидности информационных операций и атак, реализуемых в СТИС, способы их реализации в информационном пространстве.

уметь:

- анализировать и классифицировать различные виды сетевых атак, оценивать риски и защищенность от них;

владеть:

- навыками математического моделирования ИОА и приемами противодействия им.

Аннотация программы дисциплины
С3.Б.1 «Безопасность жизнедеятельности»
Трудоемкость ЗЕТ 3 (108 часов)

Цели и задачи изучения дисциплины

Основная цель состоит в сохранении работоспособности и здоровья человека за счет выбора оптимальных параметров состояния среды обитания и применения мер защиты от негативных факторов естественного и антропогенного происхождения.

Основные дидактические единицы (разделы)

Человек и среда обитания. Основы физиологии труда и комфортные условия жизнедеятельности в техносфере. Идентификация и воздействие на человека вредных и опасных факторов среды обитания. Защита человека и среды обитания от вредных и опасных факторов природного, антропогенного и техногенного происхождения. Обеспечение комфортных условий для жизни и деятельности человека. Психофизиологические и эргономические основы безопасности. Чрезвычайные ситуации и методы защиты в условиях их реализации. Управление безопасностью жизнедеятельности.

Компетенции, приобретаемые студентом в процессе изучения дисциплины ОК-1, ОК-2, ОК-6, ОК-7, ОК-8, ОК-9, ОК-10, ПК-7.

В результате изучения дисциплины студенты должны:

знать:

- опасные и вредные факторы системы «человек – среда обитания»; научные и организационные основы защиты окружающей среды и ликвидации последствий аварий, катастроф, стихийных бедствий

уметь:

реализовывать и контролировать выполнение требований по охране труда и технике безопасности в профессиональной деятельности; применять основные методы защиты производственного персонала и населения от

возможных последствий аварий, катастроф, стихийных бедствий.

владеть:

- навыками безопасного использования технических средств в профессиональной деятельности.

Аннотация программы учебной дисциплины С3.Б.2 «Языки программирования»

Трудоемкость 9 ЗЕТ (324 часа)

Цель и задачи дисциплины

Целью изучения дисциплины «Языки программирования» является подготовка специалистов к деятельности, связанной с разработкой программного обеспечения для решения профессиональных задач.

Задачи дисциплины: ознакомление с теоретическими основами программирования; изучение основ алгоритмизации; изучение средств описания данных и средств описания действий языков программирования; овладение навыками программирования; освоение современных сред создания программных продуктов.

Требования к уровню освоения содержания дисциплины

В результате изучения дисциплины студент должен **знать:**

- общие принципы построения и использования современных языков программирования высокого уровня;
- языки программирования высокого уровня (объектно-ориентированное программирование);
- возможности, классификацию и области применения макрообработки;
- способы обработки исключительных ситуаций;
- основные структуры данных и способы их реализации на языке программирования;

уметь:

- работать с интегрированной средой разработки программного обеспечения;
- использовать шаблоны классов и средства макрообработки;
- использовать динамически подключаемые библиотеки;
- реализовывать основные структуры данных и базовые алгоритмы средствами языков программирования;

владеть:

- навыками проектирования программного обеспечения с использованием средств автоматизации;
- навыками программирования с использованием эффективных реализаций структур данных и алгоритмов.

Программа направлена на реализацию следующих компетенций ПК-3; ПК-4; ПК-5, ПК-8, ПК-10.

Раздел 1. Основы языков программирования высокого уровня. Язык С/С++

Тема 1. Общая характеристика языков программирования

Тема 2. Базовые понятия языка

Тема 3. Указатели, ссылки, массивы

Тема 4. Функции

Тема 5. Типы данных, определяемые пользователем

Тема б.Ввод -вывод.Работа с файлами

Тема7.Препроцессорные средства

Тема8. Операции с разрядами

Тема9.Межпроцессное взаимодействие. Параллельное программирование.

Раздел 2. Введение в объектно-ориентированное программирование. Язык С++

Тема 10. Основные принципы объектно-ориентированного программирования.

Тема 11. Классы и объекты

Раздел3. Основы объектно-ориентированного программирования.Язык С++

Тема 12. Перегрузка операций

Тема 13. Наследование

Тема 14. Виртуальные функции и полиморфизм

Тема 15. Шаблоны классов

Тема 16. Потоковыйввод-вывод

Тема17. Обработка исключительных ситуаций

Тема18. Стандартная библиотека шаблонов^ТЬ)

Тема19. Приложения с графическим интерфейсом пользователя

Аннотация программы учебной дисциплины С3.Б.3 «Технологии и методы программирования»

Трудоемкость 8 ЗЕТ (288 часа)

- **Цель задачи дисциплины**

Целью изучения дисциплины «Технологии и методы программирования» является изучение современных технологий и методов программирования, получение навыков проектирования и разработки программного обеспечения (ПО), расширение кругозора в сфере разработки ПО.

Задачи дисциплины:

- изучение методологии и средств разработки ПО; изучение методов проектирования ПО; изучение оценки качества программного обеспечения; изучение тестирования и отладки программного обеспечения; изучение принципов, методов и средств сопровождения ПО; изучение структур данных; изучение алгоритмов и навыков их практической реализации при разработке программных систем.

- **Требования к уровню освоения содержания дисциплины**

В результате изучения дисциплины

студент должен : **знать:**

современные технологии и методы программирования;
показатели качества программного обеспечения;
методологии и методы проектирования программного обеспечения;
методы тестирования и отладки программного обеспечения;
принципы организации документирования разработки, процесса сопровождения программного обеспечения;
основные комбинаторные и теоретико-графовые алгоритмы, а также способы их эффективной реализации и оценки сложности.

уметь:

3.формировать требования и разрабатывать внешние спецификации для разрабатываемого программного обеспечения;
4.планировать разработку сложного программного обеспечения;
5.проектировать структуру и архитектуру программного обеспечения с использованием современных методологий и средств автоматизации проектирования программного обеспечения;
6.проводить комплексное тестирование и отладку программных систем;
7.проектировать и кодировать алгоритмы с соблюдением требований к качественному стилю программирования;
8. проводить выбор эффективных способов реализации структур данных и конкретных алгоритмов при решении профессиональных задач;

владеть:

- навыками разработки, документирования, тестирования и отладки программного обеспечения в соответствии с современными технологиями и методами программирования;
- навыками разработки программной документации.

Программа направлена на реализацию следующих компетенций ОК-5, ОК-9, ОК-10, ПК-1, ПК-2, ПК-3, ПК-5, ПК-8, ПК-9, ПК-10.

- Содержание дисциплины.

Раздел 1. Технология программирования
Тема 1. Жизненный цикл ПО, методологии и стандарты разработки ПО
Тема 2. Планирование и организация разработки ПО
Тема 3. Проектирование ПО
Тема 4. Основы объектно-ориентированного анализа и проектирования ПО
Тема 5. Кодирование ПО
Тема 6. Технологии разработки распределенных программных систем.Перспективы развития технологий программирования
Тема 7. Тестирование и отладка ПО
Тема 8. Документирование ПО
Тема 9. Сопровождение ПО
Раздел 2. Методы программирования
Тема 10. Методы анализа алгоритмов
Тема 11. Динамические структуры данных
Тема 12. Поиск и сортировка
Тема 13. Основные алгоритмы на графах

Аннотация программы учебной дисциплины С3.Б.4
«Электроника и схемотехника»

Трудоемкость 8 ЗЕТ (288 часов)

Цели и задачи дисциплины

Целью изучения дисциплины «Электроника и схемотехника» является теоретическая и практическая подготовка специалистов к деятельности, связанной с проектированием, разработкой и применением электронной аппаратуры для обеспечения безопасности автоматизированных систем.

Задачи дисциплины: изучение основных элементов теории электрических цепей; изучение принципов работы базовых аналоговых и цифровых электронных схем; изучение схемотехнических подходов разработки основных аналоговых и цифровых узлов автоматизированных систем; изучение методов анализа работы электронных схем; изучение принципов применения современных электронных средств обеспечения информационной безопасности автоматизированных систем; овладение методами разработки узлов автоматизированных систем на основе современной элементной базы.

Требования к результатам освоения дисциплины

В результате изучения дисциплины студент должен

знать:

- основы теории электрических цепей;
- принципы работы элементов и функциональных узлов электронной аппаратуры;
- методы анализа и синтеза электронных схем;
- типовые схемотехнические решения основных узлов и блоков электронной аппаратуры;

уметь:

- применять на практике методы анализа электрических цепей;
- работать с современной элементной базой электронной аппаратуры;
- использовать стандартные методы и средства проектирования цифровых узлов и устройств, в том числе для средств защиты информации;

владеть:

- навыками использования современной измерительной аппаратуры при экспериментальном исследовании электронной аппаратуры;
- навыками работы с программными средствами схемотехнического моделирования;
- навыками чтения принципиальных схем, построения временных диаграмм и восстановления алгоритма работы узла, устройства и системы по комплекту документации;
- навыками оценки быстродействия и оптимизации работы электронных схем на базе современной элементной базы.

Программа направлена на реализацию следующих компетенций: ОК-

9, ОК-10, ПК-1, ПК-2, ПК-8, ПК-9, ПК-10.

Содержание дисциплины

Раздел 1. Основы теории электрических цепей и сигналов

Тема 1. Основные определения и законы теории электрических цепей

Тема 2. Электрические цепи при гармоническом воздействии

Тема 3. Четырехполюсники, фильтры и длинные линии

Тема 4. Сигналы и их спектры

Раздел 2. Полупроводниковые приборы, усилители и аналоговые преобразователи

Тема 5. Полупроводниковые приборы

Тема 6. Электронные усилители

Тема 7. Нелинейное и параметрическое преобразование сигналов

Раздел 3. Схемотехника импульсных и цифровых устройств

Тема 8. Цифровая схемотехника

Тема 9. Триггеры

Тема 10. Функциональные узлы комбинационного и последовательностного типа

Раздел 4. Схемотехника запоминающих устройств и устройств на базе программируемой логики

Тема 11. Схемотехника запоминающих устройств

Тема 12. Схемотехника устройств на базе программируемой логики

Раздел 5. Разработка и применение цифровых устройств

Тема 13. Функционирование цифровых элементов в составе узлов и блоков

Тема 14. Разработка и применение цифровых узлов и блоков

Аннотация программы учебной дисциплины С3.Б.5 «Безопасность операционных систем»

Трудоемкость 8 ЗЕТ (288 часов)

Цели и задачи дисциплины

Целью преподавания дисциплины «Безопасность операционных систем» является теоретическая и практическая подготовка специалистов в области эксплуатации современных операционных систем (ОС) для обеспечения их эффективного применения с учетом требований информационной безопасности и привитие навыков в использовании методов обеспечения защиты информации в ОС.

Задачи дисциплины:

- изучение назначения и функций ОС;
- приобретение навыков управления ресурсами и задачами в ОС;
- освоение администрирования ОС;
- изучение требований к защите ОС;
- изучение методов и средств разграничения доступа в ОС;
- изучение аудита в ОС;

- формирование специальных теоретических и практических знаний, обеспечивающих возможность планирования политики безопасности ОС;
- приобретение навыков эффективной и безопасной эксплуатацию ОС автоматизированных систем;
- формирование специальных теоретических и практических знаний, обеспечивающих возможность проектировании средств защиты информации и средств контроля защищенности автоматизированных систем;
- приобретение навыков эффективного применения информационно-технологических ресурсов ОС с учетом требований информационной безопасности;
- приобретение навыков эффективного применения средств защиты информационнотехнологических ресурсов ОС;
- формирование специальных теоретических и практических знаний, позволяющих администрировать подсистему информационной безопасности автоматизированной системы;
- формирование специальных теоретических и практических знаний, позволяющих обеспечить восстановление работоспособности систем защиты информации при возникновении нештатных ситуаций.

Требования к результатам освоения дисциплины

В результате изучения дисциплины студент должен:

знать:

- принципы построения и функционирования, примеры реализаций современных операционных систем;
- функции ОС, основные концепции управления процессорами, памятью, вспомогательной памятью, устройствами;
- критерии оценки эффективности и надежности средств защиты ОС;
- принципы организации и структуру подсистем защиты ОС семейств UNIX и Windows;

уметь:

- использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем;
- оценивать эффективность и надежность защиты операционных систем;
- планировать политику безопасности операционных систем;

владеть:

- навыками работы с операционными системами семейств Windows и Unix, восстановления операционных систем после сбоев;
- навыками установки и настройки операционных систем семейств Windows и Unix с учетом требований по обеспечению информационной безопасности.

Программа направлена на реализацию следующих компетенций: ОК-1; ПК-1; ПК-2; ПК-3; ПК-19.

Содержание дисциплины

Основы функционирования ОС. Назначение и функции операционных систем. Управление задачами и ресурсами в ОС. Автоматизация решения задач администрирования в ОС с использованием языков сценариев. Безопасность ОС. Требования к защите ОС. Разграничение доступа в ОС. Аудит в ОС.

Аннотация программы учебной дисциплины С3.Б.6 «Безопасность сетей ЭВМ»

Трудоемкость 7 ЗЕТ (252 часа)

Цели и задачи дисциплины

Целью изучения дисциплины «Безопасность сетей ЭВМ» является теоретическая и практическая подготовка специалистов в области построения сетей ЭВМ и обеспечения безопасности при эксплуатации сетей ЭВМ.

Задачи:

изучение основных элементов теории построения сетей;

- изучение основных принципов функционирования сетевых протоколов;

привитие навыков комплексного проектирования, построения, обслуживания и анализа защищенных вычислительных сетей;

изучение основных угроз в сетях ЭВМ и методов противодействия им;

овладение механизмами построения систем безопасности сетей ЭВМ.

- **Требования к результатам освоения дисциплины**

В результате изучения дисциплины студент должен:

знать:

принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей;

основные протоколы компьютерных сетей;

последовательность и содержание этапов построения компьютерных сетей;

эталонную модель взаимодействия открытых систем;

основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в компьютерных сетях;

уметь:

проектировать и администрировать компьютерные сети, реализовывать политику безопасности компьютерной сети;

эффективно использовать различные методы и средства защиты информации для компьютерных сетей;

проводить мониторинг угроз безопасности компьютерных сетей;

владеть:

навыками, эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности;

навыками разработки, документирования компьютерных сетей с учетом требований по обеспечению безопасности;

навыками использования программно-аппаратных средств обеспечения безопасности компьютерных сетей.

Программа направлена на реализацию следующих компетенцией: ОК-1; ОК-9; ПК-13; ПК-15.

Содержание дисциплины

Безопасность сетезависимых уровней. Основы организации и функционирования сетей ЭВМ. Физический и канальный уровень построения сетей ЭВМ. Технологии построения локальных сетей ЭВМ. Сетевой уровень построения сетей ЭВМ. Маршрутизация. Транспортная подсистема сетей ЭВМ. Программно-технические средства защиты сетей ЭВМ.

Аннотация программы учебной дисциплины С3.Б.7 «Безопасность систем баз данных»

Трудоемкость 6 ЗЕТ (216 часов)

Цели и задачи дисциплины

Целью преподавания дисциплины "Безопасность систем баз данных" является подготовка специалистов в области разработки и эксплуатации систем баз данных с учетом требований по обеспечению информационной безопасности.

В задачи дисциплины "Безопасность систем баз данных" входит формирование необходимого минимума специальных теоретических знаний и практических навыков по следующим аспектам: проектирование баз данных; разработка прикладных программ для систем баз данных; эксплуатация систем баз данных; обеспечение информационной безопасности систем баз данных.

Требования к результатам освоения дисциплины

В результате изучения дисциплины

студент должен **знать:**

- принципы построения и функционирования, архитектуру, примеры реализаций современных систем управления базами данных;
- основные модели данных, физическую организацию баз данных;
- средства обеспечения безопасности данных;
- последовательность и содержание этапов

проектирования баз данных; **уметь:**

- разрабатывать и администрировать базы данных и интерфейсы прикладных программ к базам данных;
- реализовывать политику безопасности баз данных;
- выделять сущности и связи предметной области;
- отображать предметную область на конкретную модель данных;
- нормализовать отношения при проектировании реляционной базы данных;
- создавать объекты базы данных;

- выполнять запросы к базе данных;
- разрабатывать прикладные программы, осуществляющие взаимодействие с базами данных;
- применять средства обеспечения безопасности данных; **владеть:**
- навыками эксплуатации и администрирования баз данных с учетом требований по обеспечению информационной безопасности;
- навыками разработки, документирования баз данных с учетом требований по обеспечению информационной безопасности.

Программа направлена на реализацию следующих компетенций: ПК-8, ПК-9, ПК-10.

Содержание дисциплины

Раздел 1. Основы систем баз данных

Тема 1. История развития, назначение и роль систем баз данных

Тема 2. Основы теории баз данных

Тема 3. Реляционные базы данных

Тема 4. Проектирование баз данных

Тема 5. Физическая организация баз данных

Тема 6. Средства поддержания интерфейса с различнымикатегориями пользователей

Тема 7. Концепция безопасности баз данных

Тема 8. Средства обеспечения целостности баз данных

Тема 9. Средства обеспечения конфиденциальности баз данных

Тема 10. Аудит систем баз данных

Тема 11. Средства поддержки высокой готовности систем баз данных

Аннотация программы учебной дисциплины С3.Б.8 «Основы информационной безопасности»

Трудоемкость 4 ЗЕТ (144 часа)

Цели и задачи дисциплины

- Целью изучения дисциплины является ознакомление студентов с основными понятиями информационной безопасности, классификацией систем и средств, обеспечивающих информационную безопасность, местом и значимостью информационных технологий в системе национальной безопасности Российской Федерации.
- Основной задачей изучения дисциплины является знакомство с технологиями информационной безопасности, овладение методами управления информационными ресурсами, обеспечивающими сохранность и защиту информации в современных автоматизированных системах их обработки и хранения.

Являясь общепрофессиональной дисциплиной, данный курс вводит

студентов в главную область специализации и должен служить основой для дальнейшего освоения технологий информационной безопасности студентом, который может занимать непосредственно после окончания вуза должность специалиста по защите информации.

• Требования к результатам освоения дисциплины

В результате изучения курса согласно требованиям государственного образовательного стандарта студенты должны:

Знать:

сущность и понятие информации, информационной безопасности и характеристику ее составляющих;

место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России;

источники и классификацию угроз информационной безопасности;

основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;

основные задачи и понятия криптографии;

технические каналы утечки информации;

возможности технических средств перехвата информации;

способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации;

организацию защиты информации от утечки по техническим каналам на объектах информатизации;

основы физической защиты объектов информатизации;

основные характеристики сигналов электросвязи, спектры и виды модуляции;

основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации;

правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны и служб защиты информации на предприятиях;

программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, компьютерных сетях;

основные угрозы безопасности информации и модели нарушителя в автоматизированных системах;

Уметь:

классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;

- классифицировать и оценивать угрозы информационной безопасности для объекта информатизации;

Владеть:

профессиональной терминологией в области информационной безопасности;

методами оценки информационных рисков;

криптографической терминологией.

Программа направлена на реализацию следующих компетенций: ОК-5, ОК-9, ПК-1, ПК-13, ПК-20.

Содержание дисциплины

Цели и задачи защиты информации. Модель информационной безопасности. Правовая защита конфиденциальной информации. Организационная защита информации. Инженерно-техническая защита информации. Аппаратные средства защиты информации. Программные средства защиты информации. Криптографические средства защиты информации. Способы защиты информации в ЭВМ. Защита информации от утечки по техническим каналам. Защита от утечки по электромагнитным каналам. Противодействие несанкционированному доступу к источникам конфиденциальной информации

Аннотация программы учебной дисциплины С3.Б.9 «Криптографические методы защиты информации»

Трудоемкость 5 ЗЕТ (180 часов)

Цель изучения дисциплины «Криптографические методы защиты информации» - дать студентам общие сведения и представления о методах и средствах обеспечения безопасности информации в современных автоматизированных системах на основе криптографии.

Основными задачами дисциплины являются:

дать студентам основы системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами, на основе применения криптографических методов;

дать студентам основы принципов анализа и синтеза шифров;

ознакомить студентов с математическими методами, используемыми в криптографии.

Требования к результатам освоения дисциплины

В результате изучения дисциплины студент должен:

знать:

- основные задачи и понятия криптографии;
- требования к шифрам и основные характеристики шифров;
- типовые поточные и блочные шифры;
- частотные характеристики открытых текстов и способы их применения к анализу простейших шифров замены и перестановки;
- типовые шифры с открытыми ключами;
- модели шифров и математические методы их исследования;
- основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в компьютерных сетях;

уметь:

- эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах;
- применять математические методы исследования моделей шифров;

владеть:

- криптографической терминологией;
- навыками использования типовых криптографических алгоритмов;
- навыками использования ЭВМ в анализе простейших шифров;
- навыками математического моделирования в криптографии.

Программа направлена на реализацию следующих компетенций: ПК-23; ПК-30; ПК-36.

Содержание дисциплины

Раздел 1. Основные понятия криптографии.

Раздел 2. Виды информации, подлежащие закрытию, ее модели и свойства.

Раздел 3. Принципы построения криптографических алгоритмов.

Раздел 4. Криптографические хеш-функции.

Раздел 5. Поточные шифры и генераторы псевдослучайных чисел.

Раздел 6. Системы шифрования с открытыми ключами.

Раздел 7. Криптографическая стойкость шифров.

Заключение. Основные направления и перспективы развития криптографических средств защиты информации.

Аннотация программы учебной дисциплины С3.Б.10
Организация ЭВМ и вычислительных систем

Трудоемкость 6 ЗЕТ (216 часов)

1. Цели и задачи дисциплины

Целью преподавания дисциплины «Организация ЭВМ и вычислительных систем» является теоретическая и практическая подготовка специалистов в области эксплуатации современных ЭВМ и привитие навыков в использовании вычислительных систем.

Задачи дисциплины:

- изучение элементов и узлов ЭВМ;
- изучение структуры центрального процессора;
- изучение функций и назначения периферийных устройств ЭВМ;
- приобретение навыков работы с вычислительными системами;
- изучение общей структуры микропроцессора;
- изучение архитектуры современных ЭВМ;
- приобретение навыков работы с рабочими станциями и серверами;
- формирование специальных теоретических и практических знаний, обеспечивающих возможность проектирования объектно-ориентированной архитектуры;

Требования к результатам освоения дисциплины

В результате изучения дисциплины студент должен:

Знать:

- архитектуру, принципы функционирования, элементарную базу современного персонального компьютера, вычислительные и телекоммуникационные системы;
- терминологию, основные руководящие и регламентирующие документы в области ЭВМ, комплексов и систем;
- технические характеристики, показатели качества ЭВМ и систем, методы их оценки и пути совершенствования;

Уметь:

- проводить анализ архитектуры и структуры ЭВМ и систем, оценивать эффективность архитектурно-технических решений, реализованных при построении ЭВМ и систем;
- осуществлять сбор, обработку, анализ и систематизацию научно-технической информации в области ЭВМ и систем с применением современных информационных технологий;

Владеть:

- методиками оценки показателей качества и эффективности ЭВМ и вычислительных систем;
- навыками работы с технической документацией на ЭВМ и вычислительных системах.

Программа направлена на реализацию следующих компетенций: ПК-15; ПК-18; ПК-23.

Содержание дисциплины, основные разделы

Способы представления и преобразования сообщений, сигналов и помех. Общие сведения о системах связи. (информация. сообщение. сигнал, обобщенная структура систем связи, дискретизация непрерывного сигнала). Методы модуляции в системах связи. Цифровая обработка аналоговых сигналов. (преобразование аналог—цифра. шумы квантования, преобразование цифра-аналог и восстановление континуального сигнала)назначение и классификация кодов, (неравномерные эффективные коды, принципы помехоустойчивого кодирования, линейные двоичные блочные коды, циклические коды, сверточные коды) уплотнение информации в аналоговых системах связи. Цифровые системы многоканальной передачи.

Аннотация программы учебной дисциплины С3.Б.11 «Техническая защита информации»

Трудоемкость 4 ЗЕТ (144 часа)

Цели и задачи дисциплины

Целью дисциплины «Техническая защита информации» является теоретическая и практическая подготовка студентов по вопросам защиты информации от утечки по техническим каналам (технической защиты информации) на объектах информатизации и в выделенных помещениях.

Задачами дисциплины является изучение технических каналов утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами; технических каналов утечки акустической

(речевой) информации; способов и средств защиты информации, обрабатываемой техническими средствами; способов и средств защиты выделенных (защищаемых) помещений от утечки акустической (речевой) информации; методов и средств контроля эффективности защиты информации от утечки по техническим каналам; основ организации технической защиты информации на объектах информатизации.

Требования к результатам освоения дисциплины

В результате изучения дисциплины «Техническая защита информации» студенты должны:

знать.

технические каналы утечки информации;

возможности технических средств перехвата информации;

способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации;

организацию защиты информации от утечки по техническим каналам на объектах информатизации;

основы физической защиты объектов информатизации;

основные характеристики сигналов электросвязи, спектры и виды модуляции;

уметь :

анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем;

пользоваться нормативными документами по противодействию технической разведке;

анализировать и оценивать угрозы информационной безопасности объекта;

применять знания о системах электрической связи для решения задач по созданию защищенных телекоммуникационных систем

владеть:

методами и средствами технической защиты информации;

методами расчета и инструментального контроля показателей технической защиты информации.

Программа направлена на реализацию следующих компетенций: ПК-8; ПК-14; ПК-36.

Содержание дисциплины

Раздел 1. Технические каналы утечки информации

Тема 1. Основные понятия и определения

Тема 2. Технические каналы утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами

Тема 3. Технические каналы утечки акустической (речевой) информации

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

Тема 1. Способы и средства защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами

Тема 2. Способы и средства защиты выделенных помещений от утечки речевой информации по техническим каналам

Раздел 3. Методы и средства контроля эффективности технической защиты информации

Тема 1. Методы и средства контроля эффективности технической защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами

Тема 2. Методы и средства контроля эффективности защиты выделенных помещений от утечки речевой информации по техническим каналам

Тема 3. Методы и средства выявления электронных устройств негласного получения информации

Раздел 4. Организация технической защиты информации

Тема 1. Основы физической защиты объектов информатизации.

Тема 2. Организация технической защиты информации на объектах информатизации

Аннотация программы учебной дисциплины С3.Б.12
Сети и системы передачи информации

Трудоемкость 8 ЗЕТ (288 часов)

Цели и задачи дисциплины

Дисциплина «Сети и системы передачи информации» имеет целью обучение принципам построения и эксплуатации различных телекоммуникационных сетей и систем за счет изучения современных телекоммуникационных технологий и технических средств.

Задачи дисциплины:

- изучение базовой эталонной модели взаимосвязи открытых систем;
- изучение современных телекоммуникационных технологий, применяемых при построении телекоммуникационных сетей и систем;
- изучение современных технических средств, применяемых при построении телекоммуникационных сетей и систем;
- обучение методам компьютерного моделирования работы телекоммуникационных сетей и систем.

Требования к результатам освоения дисциплины

В результате изучения дисциплины студенты должны:

знать:

- основные характеристики сигналов электросвязи, спектры и виды модуляции;
- принципы построения и функционирования систем и сетей передачи информации;
- способы кодирования информации;
- основные телекоммуникационные протоколы.

уметь:

- применять знания о системах электрической связи для решения задач по созданию защищенных телекоммуникационных систем;
- анализировать тенденции развития систем и сетей электросвязи, внедрения новых служб и услуг связи.

владеть:

- навыками анализа основных характеристик и возможностей телекоммуникационных систем по передаче информации.

Программа направлена на реализацию следующих компетенций:

ПК-1; ПК-8; ПК-18.

Содержание дисциплины

Раздел 1. Основы сетей и систем передачи информации.

Раздел 2. Технологии физического уровня.

Раздел 3. Локальные вычислительные сети.

Раздел 4. Сети TCP/IP.

Раздел 5. Технологии глобальных сетей.

Аннотация программы учебной дисциплины С3.Б.13 Организационное и правовое обеспечение информационной безопасности

Трудоемкость 4 ЗЕТ (144 часа)

Цель дисциплины: Приобретение студентами знаний по организационному обеспечению защиты информации и формирование практических навыков работы в конкретных условиях, необходимых для комплексного обеспечения безопасности информации. Обеспечение основ правовой подготовки бакалавров в области защиты информации, развитие навыков работы с нормативно-правовыми документами, приобретение знаний и навыков, необходимых для комплексного обеспечения.

Задачи дисциплины:

- Изучение теоретических, методологических и практических проблем формирования и развития систем организационной защиты информации, а также получение практических навыков использования полученных знаний для защиты информации ограниченного доступа.
- Овладение теоретическими и практическими навыками использования правовых принципов и норм для защиты информации, ознакомление с основными нормативно-правовыми документами, регулирующими

отношения в информационной сфере и сфере защиты информации, получения навыков использования правовых знаний для защиты информации ограниченного доступа.

Требования к результатам освоения дисциплины:

Компетенции, формируемые в результате освоения дисциплины ОК-1 — способностью осознавать необходимость соблюдения Конституции Российской Федерации,прав и обязанностей гражданина своей страны, гражданского долга и проявления патриотизма; ОК-6 — способностью находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность; ПК-24 — способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности;ПК-3 — способностью использовать нормативные правовые документы в своей профессиональной деятельности; ПК-33 — способностью организовать технологический процесс защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю; ПК-4 — способностью формировать комплекс мер по информационной безопасности с учётом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности;ПК-5 — способностью организовывать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учётом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации; ПК-6 — способностью организовать проведение и сопровождать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов.

В результате освоения дисциплины студент должен:

знать:

- теоретические основы функционирования систем организационной защиты информации, её современные проблемы и терминологию;
- цели, функции и процессы управления системами организационной защиты информации в организациях с различными формами собственности;
- основные направления и методы организационной защиты информации;
- структуру и логику построения нормативно-правовых документов;
- терминологию и основные понятия, используемые законодателем для регулирования правоотношений в информационной сфере и сфере защиты информации;
- правовые принципы, нормы и методы, используемые при регулировании правоотношений защите информации;
- существующую в России систему правовой защиты информации;
- основные разделы права, регулирующие имущественные и

неимущественные отношения применимые для защиты информации;

- группу специальных нормативно-правовых актов, включающих Федеральные законы, законов субъектов РФ, подзаконные акты, и распорядительные документы регулирующие отношения по защите информации;
- виды информации ограниченного доступа и особенности их правовой защиты;
- права и особенности субъектов сферы защиты информации ограниченного доступа;
- законодательно закрепленные виды угроз информационной безопасности и требование по защите информации;
- порядок лицензирования и сертификации в сфере защиты информации;
- особенности правовой защиты информации, составляющей интеллектуальную собственность;
- правовые санкции, применяемые к нарушителям требований правовых норм по защите информации.

уметь:

- анализировать эффективность систем организационной защиты информации и разрабатывать направления её развития;
- разрабатывать нормативно-методические материалы по регламентации системы организационной защиты информации;
- организовывать работу с персоналом, обладающим конфиденциальной информацией;
- организовывать охрану персонала, территорий, зданий, помещений и продукции организаций;
- организовывать и проводить служебное расследование по фактам разглашения, утечки информации и несанкционированного доступа к ней;
- организовывать и проводить аналитическую работу по предупреждению утечки конфиденциальной информации;
- пользоваться законами, подзаконными актами, распорядительной для поиска и использования в работе необходимой правовой информации;
- взаимодействовать с представителями органов государственной власти, правоохранительных, судебных и фискальных органов, а также органов лицензирования и сертификации;
- учитывать в практической деятельности особенности установления режимов правовой охраны информации для различноговида тайн;
- формировать политику безопасности предприятия и организации с учётом правовой составляющей;
- юридически обоснованно подготавливать распорядительные документы по поддерживанию режима правовой охраны информации с ограниченным доступом;

- устанавливать особый порядок защиты персональных данных;
- участвовать в разработке мер по защите интеллектуальной собственности;
- давать правовую оценку взаимоотношениям работодателя и работника по вопросам защиты информации.

владеть: практическими навыками использования организационных и правовых принципов и норм для защиты информации.

Содержание дисциплины:

1. Понятие «Организационная защита информации».
2. Организационные источники и каналы утечки информации. Силы, средства и условия организационной защиты информации.
3. Особенности системы организационной защиты информации, составляющей государственную и коммерческую тайну.
4. Порядок засекречивания и рассекречивания конфиденциальных сведений, документов и изделий.
5. Подбор персонала на должности, связанные с работой с конфиденциальной информацией.
6. Допуск к информации ограниченного доступа.
7. Организация доступа к информации.
8. Текущая работа с персоналом, обладающим конфиденциальной информацией.
9. Организация служебного расследования по фактам разглашения персоналом конфиденциальной информации.
10. Организация охраны территории, зданий, помещений и персонала.
11. Организация пропускного и внутриобъектового режимов.
12. Требования к помещениям и хранилищам в которых ведутся закрытые работы и хранятся конфиденциальные документы и изделия.
13. Организация подготовки и проведения совещаний и переговоров по конфиденциальным вопросам.
14. Организация защиты информации при приеме в организации посетителей и командированных лиц.
15. Организация защиты информации при приеме в организации иностранных представителей.
16. Организация защиты информации при осуществлении рекламной и выставочной деятельности.
17. Организация защиты информации при подготовке материалов к открытому опубликованию.
18. Аналитическая работа как основа управления системой организационной защиты информации.
19. Планирование процессов организационной защиты информации.
20. Контроль функционирования системы организационной защиты информации.
21. Характеристика правоотношений в сфере защиты информации.

22. Структура системы организационно-правового обеспечения информационной безопасности в России.

23. Содержание основных нормативно-правовых актов, направленных на защиту информации ограниченного доступа.

24. Правовой порядок установления и поддержание режимаограничения доступа к информации.

25. Лицензирование и сертификация, как методы правового регулирования отношений в сфере защиты информации.

26. Правовые последствия введения режима ограниченния доступа для субъектов защиты информации. Сферы.

27. Государственная система правовой защиты сведений, составляющих государственную тайну.

28. Особенности правовой защиты сведений, составляющих различные виды тайн.

29. Правовая защита информации, составляющей интеллектуальную собственность.

30. Правовое обеспечение безопасности информационных и телекоммуникационных систем.

Аннотация программы учебной дисциплины С3.Б.14
«Программно-аппаратные средства
обеспечения информационной безопасности»

Трудоемкость 3 ЗЕТ (108 часов)

- **Цели и задачи дисциплины**

Целью преподавания дисциплины «Программно-аппаратные средства обеспечения информационной безопасности» является подготовка специалистов в области проектирования средств обеспечения информационной безопасности автоматизированных систем и привитие навыков разработки и анализа компонентов автоматизированных систем.

Задачи дисциплины:

изучение моделей угроз и модели нарушителя информационной безопасности автоматизированной системы;

изучение методов анализа проектных решений по обеспечению безопасности автоматизированных систем;

получение практических навыков проектирования средств защиты информации автоматизированной системы;

изучение методов анализ угроз и уязвимостей проектируемых и эксплуатируемых автоматизированных систем;

получение навыков использования программно-аппаратных средств обеспечения безопасности сетей автоматизированных систем.

- **Требования к результатам освоения дисциплины**

В результате изучения дисциплины студент должен:

знать:

программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, компьютерных сетях**;**

уметь:

проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы;

разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем;

владеть:

навыками, эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности;

навыками использования программно-аппаратных средств обеспечения безопасности сетей ЭВМ.

Программа направлена на реализацию следующих компетенций: ОК-9, ПК-9, ПК-36.

- **Содержание дисциплины**

Назначение и функции программно-аппаратных средств обеспечения безопасности. Методы защиты информации от несанкционированного доступа. Методы обеспечения целостности аппаратного обеспечения автоматизированных систем. Анализ уязвимости программного обеспечения автоматизированных систем. Методы защиты от вредоносных программ. Средства идентификация и аутентификации пользователей автоматизированных систем.

Аннотация программы учебной дисциплины С3.Б.15 «Разработка и эксплуатация защищенных автоматизированных систем»

Трудоемкость 4 ЗЕТ (144 часа)

- **Цели и задачи дисциплины**

Целью изучения дисциплины «Разработка и эксплуатация защищенных автоматизированных систем» является теоретическая и практическая подготовка специалистов к деятельности, связанной с разработкой и эксплуатацией защищенных автоматизированных информационных систем в своей профессиональной деятельности.

Задачи дисциплины:

изучение методов и средств разработки автоматизированных систем и подсистем безопасности автоматизированных систем;

изучение содержания основных этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем;

изучение методов, способов и средств обеспечения отказоустойчивости автоматизированных систем;

изучение основных мер по защите информации в автоматизированных системах;

овладение навыками эксплуатации автоматизированных информационных систем для решения различных классов задач;

формирование у обучаемых научного подхода к осмыслению процессов обработки, хранения и передачи информации.

- **Требования к результатам освоения дисциплины**

В результате изучения дисциплины студент должен

знать:

основные информационные технологии, используемые в автоматизированных системах;

основные угрозы безопасности информации и модели нарушителя в автоматизированных системах;

автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности;

методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности

автоматизированных систем;

содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем;

методы, способы и средства обеспечения отказоустойчивости автоматизированных
систем;

- основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические);

основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения информационной безопасности в автоматизированных и телекоммуникационных системах;

уметь:

разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем;

администрировать подсистемы информационной безопасности автоматизированных систем;

восстанавливать работоспособность подсистемы информационной безопасности автоматизированных систем в нештатных ситуациях;

- исследовать эффективность создаваемых средств автоматизации, проводить технико-экономическое обоснование проектных решений;

разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов;

определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите;

разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем;

выявлять уязвимости информационно-технологических ресурсов автоматизированных систем, проводить мониторинг угроз безопасности автоматизированных систем

владеть:

навыками анализа основных узлов и устройств современных автоматизированных систем;

навыками поддержания работоспособности, обнаружения и устранения неисправностей в работе электронных аппаратных средств автоматизированных систем;

методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем;

навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем;

навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем.

Программа направлена на реализацию следующих компетенций: ПК-10; ПК-12; ПК-14; ПК-16; ПК-33.

- Содержание дисциплины

Разработка защищенных автоматизированных систем. Защищенные АИС. Основные понятия и классификация. Основы организации разработки защищенных АИС. Общие принципы проектирования защищенных АИС. Эксплуатация защищенных автоматизированных систем. Основы эксплуатации защищенных АИС. Диагностика программных и аппаратных средств АИС.

Аннотация программы учебной дисциплины С3.Б.16 «Управление информационной безопасностью»

Трудоемкость 4 ЗЕТ (144 часа)

Цели и задачи дисциплины

Дисциплина "Управление информационной безопасностью" имеет целью изучение основных понятий, методологии и практических приемов управления технической и организационной инфраструктурой обеспечения информационной безопасности на предприятии.

Задачами дисциплины являются:

-приобретение обучаемыми необходимого объема знаний и практических навыков в области стандартизации и нормотворчества в управлении информационной безопасностью, оценки рисков информационных ресурсов предприятия и аудита информационной безопасности, организации работы и разграничения полномочий персонала, ответственного за информационную безопасность;

-формирование у обучаемых целостного представления об организации и содержании процессов управления информационной безопасностью на предприятии как результата внедрения системного подхода к решению задач обеспечения информационной безопасности (ИБ) автоматизированных систем (АС).

Требования к результатам освоения дисциплины

В результате изучения дисциплины

студент должен **знать:**

-основные методы управления информационной безопасностью;

-методы аттестации уровня защищенности автоматизированных систем;

-основные положения стандартов Единой системы конструкторской документации, Единой системы программной документации;

-принципы формирования политики информационной безопасности в автоматизированных системах;

уметь:

- оценивать информационные риски в автоматизированных системах;
- определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем;
- составлять аналитические обзоры по вопросам обеспечения информационной безопасности автоматизированных систем;
- разрабатывать частные политики информационной безопасности автоматизированных систем;
- контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем;
- разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем;
- применять требования Единой системы конструкторской документации и Единой системы программной документации при разработке технической документации;

владеть:

-навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности;

-методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем;

-методами управления информационной безопасностью автоматизированных систем; -методами оценки информационных рисков;

-навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем;

-навыками участия в экспертизе состояния защищенности информации на объекте защиты.

Программа направлена на реализацию следующих компетенций: ПК-21; ПК-29; ПК-33; ПК-39.

Содержание дисциплины

Система управления информационной безопасностью автоматизированных систем. Политика безопасности автоматизированных систем. Организация обеспечения информационной безопасности автоматизированных систем. Аудит информационной безопасности автоматизированных систем. Средства поддержки процессов управления информационной безопасностью АС

Аннотация к рабочей программе дисциплины «Инженерная графика»

Трудоемкость 2 ЗЕТ (72 часа)

Целями освоения учебной дисциплины являются: развитие навыков инженерного мышления, обучение применению инженерных навыков и основ инженерного и компьютерного моделирования в практической деятельности.

Задачами курса являются: формирование целостного представления об основных этапах становления современной инженерной и компьютерной графики, обучение приемам и принципам построения инженерных и компьютерных моделей и их использованию в профессиональной деятельности.

Краткое содержание дисциплины:

Элементы начертательной геометрии

Правила выполнения конструкторской документации

Основные команды Компаса и выполнение чертежей в 2D и 3D графике.

В результате изучения дисциплины специалист должен обладать следующими профессиональными компетенциями:

ОК-1, ОК-12, ПК-7, ПК-10.

Аннотация программы учебной дисциплины С3.Б.18 «Информационная безопасность распределенных информационных систем»

Трудоемкость 4 ЗЕТ (144 часа)

Цели и задачи дисциплины

Цель изучения дисциплины «Обеспечение информационной безопасности распределенных информационных систем» - подготовка студентов по специальности 10.05.03 «Информационная безопасность автоматизированных систем» в области теоретических основ проектирования современных защищенных автоматизированных систем. Это достигается обучением студентов принципам обеспечения информационной безопасности распределенных информационных систем.

Основными задачами дисциплины являются:

сформировать необходимый минимум специальных теоретических и практических знаний в области обеспечения информационной безопасности распределенных информационных систем.

Требования к результатам освоения дисциплины

В результате изучения дисциплины студент должен:

знать

- основные положения теории управления;
- способы обеспечения информационной безопасности систем организационного управления;
- принципы построения распределенных систем и объектно-ориентированных систем управления базами данных, CASE-технологии для проектирования баз данных и хранилищ данных, требования к архитектуре информационных систем и их компонентам для обеспечения безопасности функционирования;
- нормативные документы по метрологии, стандартизации и сертификации программных и аппаратных средств защиты.

уметь

- разрабатывать модели систем организационного управления;
- применять нормативные документы по метрологии, стандартизации и сертификации на практике;
- осуществлять согласование совместного функционирования разнородных информационных систем связи;
- оценивать эффективность защищенности распределенных информационных систем.

владеть

- навыками разработки политики безопасности систем организационного управления;
- навыками семантического моделирования данных, навыками проектирования информационных систем на базе корпоративных систем управления базами данных, методами снижения угроз безопасности информационных систем, вызванных ошибками на этапе проектирования, разработки и внедрения;
- навыками разработки документации по метрологии, стандартизации и сертификации программных и аппаратных средств защиты.

Программа направлена на реализацию следующих компетенций: ПК-15, ПСК-7.2, ПСК-7.3, ПСК-7.4, ПСК-7.5, ПСК-7.6, ПСК-7.7, ПСК-7.8.

Содержание дисциплины

Проблемно-ориентированные распределенные информационные системы. Угрозы безопасности распределенным информационным системам. Понятие безопасности распределенных информационных систем. Математическая теория криптографических преобразований. Методы обеспечения помехозащищенности и конфиденциальности информации в распределенных информационных системах. Методы поддержания эталонного состояния вычислительной среды информационной системы. Программные средства обеспечения безопасности информационных систем. Методы и инструментальные средства создания программного обеспечения. Методы и средства защиты информации от несанкционированного доступа в акустическом, электромагнитном и оптическом диапазонах.

Аннотация программы учебной дисциплины С3.Б.19 «Методы проектирования защищенных распределенных информационных систем»

Трудоемкость 4 ЗЕТ (144 часа)

1. Цели и задачи дисциплины

1.1 Целью изучения дисциплины является усвоение студентами основных принципов проектирования защищенных автоматизированных систем обработки данных, овладение методами управления проектами, обеспечивающими сохранность и защиту информации в современных компьютерных сетях и других видах автоматизированных систем.

1.2 Основными задачами изучения дисциплины являются знакомство студентов с общими принципами проектирования систем защиты

информации и привитие некоторых практических навыков в области разработки документации программно-аппаратных средств защиты информации в автоматизированных системах обработки данных, функционирующих в рамках одного предприятия (организации). Являясь специальной дисциплиной, данный курс готовит студентов к конкретным вопросам профессиональной деятельности и должен служить основой для практической проектно-конструкторской деятельности.

2. Требования к уровню освоения содержания дисциплины

В результате изучения дисциплины студент должен:

знать:

специфику математического моделирования организационных задач в автоматизированных системах; - способы обеспечения информационной безопасности систем организационного управления;- принципы построения распределенных систем и объектно-ориентированных систем управления базами данных, CASE-технологии для проектирования баз данных и хранилищ данных, требования к архитектуре информационных систем и их компонентам для обеспечения безопасности функционирования;- нормативные документы по метрологии, стандартизации и сертификации программных и аппаратных средств защиты

Уметь:

использовать CASE-технологии и структурный подход при проектировании информационных систем, определять ресурсы, необходимые для обеспечения безопасности информационной системы, использовать методы и средства определения технологической безопасности функционирования распределенной информационной системы;

- применять нормативные документы по метрологии, стандартизации и сертификации на практике

Владеть:

навыками семантического моделирования данных, навыками проектирования информационных систем на базе корпоративных систем управления базами данных, методами снижения угроз безопасности информационных систем, вызванных ошибками на этапе проектирования, разработки и внедрения;

- навыками разработки документации по метрологии, стандартизации и сертификации программных и аппаратных средств защиты.Программа направлена на реализацию следующих компетенций: ОК-10, ПК-3, ПК-22.

3. Содержание дисциплины

1.Цели и задачи технологии проектирования защищенных автоматизированных систем.

2. Синтез структуры системы передачи и обработки информации.

3. Проектирование качественной и эффективной компьютерной системы.

4 Проектирование функциональной схемы защищенных автоматизированных систем;

принципы построения защищенных информационных систем.

5. Проектирование технологического цикла реализации защищенной

системы обработки и хранения информации.

6. Организация работ по проектированию защищенных систем, функции заказчиков и разработчиков; практические методы реализации моделей безопасности; ядра безопасности; мониторинг взаимодействий в системе.

Аннотация программы учебной дисциплины С3.Б.20 «Технология построения защищенных распределенных приложений»

Трудоемкость 4 ЗЕТ (144 часа)

Цели и задачи дисциплины

Дисциплина «**Технология построения защищённых распределённых приложений**» имеет целью обучение методам проектирования и разработки защищенных распределенных приложений, соответствующим требованиям нормативных документов.

Задачи дисциплины:

• изучение нормативных документов по организации жизненного цикла, обеспечению функциональной и информационной безопасности разрабатываемых приложений;

• освоение методов обеспечения взаимодействия распределенных компонент разрабатываемых приложений;

• освоение методов обеспечения безопасности разрабатываемых приложений.

Требования к результатам освоения дисциплины

В результате изучения дисциплины студенты должны:

знать:

- нормативные документы по метрологии, стандартизации и сертификации программных и аппаратных средств защиты.

уметь:

- использовать технологии автоматизированного проектирования и структурный подход при проектировании информационных систем, определять ресурсы, необходимые для обеспечения безопасности информационной системы, использовать методы и средства определения технологической безопасности функционирования распределенной информационной системы;

- применять нормативные документы по метрологии, стандартизации и сертификации программных и аппаратных средств защиты.

владеть:

методами снижения угроз безопасности информационных систем, вызванных ошибками на этапе проектирования, разработки и внедрения.

Программа направлена на реализацию следующих компетенций:

ПСК-7.1; ПСК-7.5.

Содержание дисциплины

Раздел 1. Основы построения защищенных распределенных приложений.

Раздел 2. Взаимодействие компонент распределенных приложений.

Раздел 3. Обеспечение безопасности распределенных приложений.

Аннотация программы дисциплины
С3.В.ОД.1 «Информационные операции и атаки в распределенных информационных системах»

Трудоемкость 11 ЗЕТ (396 часов)

Цели и задачи изучения дисциплины

Основная цель состоит в исследовании информационных операций и атак, реализуемых в РИС, в контексте обеспечения их информационной безопасности. На основе анализа сущности данных систем рассматриваются организационно-правовые аспекты противодействия подобным операциям в информационно-психологическом пространствах.

Основные дидактические единицы (разделы)

Социотехнические системы как среда реализации информационных операций и атак. Специфика реализаций информационных операций и атак в РИС. Организационные аспекты в контексте информационных операций и атак в РИС. Правовые аспекты в контексте информационных операций и атак в РИС. Организационно-правовые аспекты обеспечения безопасности социотехнических систем в условиях противодействия информационным операциям и атакам в РИС.

Компетенции, приобретаемые студентом в процессе изучения дисциплины ПСК-7.1, ПСК-7.2, ПСК-7.3, ПСК-7.4, ПСК-7.5, ПСК-7.6, ПСК-7.7, ПСК-7.8, ПСК-7.9.

В результате изучения дисциплины студенты должны:

знать:

организационный механизм информационных операций и атак в РИС; структуру, субъекты применения, объекты назначения , предметы воздействия информационного оружия в РИС

уметь:

предложить формализованное представление мероприятий по планированию, подготовке, проведению информационных операций и атак в РИС; определить их топологию в РИС

владеть:

навыками анализа системой правовой проекции организационного механизма информационных операций и атак в РИС; организационно-правовыми основами обеспечения безопасности в РИС при реализации информационных операций и атак в РИС.

Аннотация программы дисциплины
С3.В.ОД2 «Социальные сети: риски и обеспечение безопасности»

Трудоемкость 13 ЗЕТ (468 часов)

1. Цели и задачи изучение дисциплины:

Основная цель изучения данной дисциплины заключается в ознакомлении с проблемой социальных сетей с точки зрения повышения

защищённости пользователей путём анализа моделей распространения вредоносного программного обеспечения, а также с помощью построения риск-моделей информационно-психологического воздействия на пользователей социальных сетей.

Задачи дисциплины связаны со способностью управлять информационными рисками и прогнозировать эффективность защиты распределенных информационных систем, подвергающихся деструктивному воздействию.

2. Основные дидактические единицы (разделы):

Социальная сеть как объект защиты от вредоносного ПО. Социальная сеть как инструмент информационного противоборства. Меры и средства защиты от атак на социальную сеть, связанных с воздействием вредоносного ПО. Аналитическое моделирование процесса заражения компьютеров пользователей СИС. Аналитическое моделирование процесса информационно-психологического воздействия на пользователей социальных сетей. Оценка эффективности применения комплексов мер противодействия угрозам воздействия вредоносного ПО и информационно-психологического воздействия на пользователей социальных сетей.

Компетенции, приобретаемые студентом в процессе изучения дисциплины: ПК-13, ПК-14, ПСК-7.2

3. В результате изучения дисциплины студенты должны:

знать:

- основные уязвимости социальных сетей для атак вредоносного ПО и информационно-психологического воздействия на пользователей;
- опасные и вредоносные факторы воздействия на элементы социальных сетей и пользователей;
- основные виды ущерба при реализации атак и воздействии на пользователей социальных сетей;

уметь:

- применять основные меры и средства защиты социальных сетей от атак вредоносного ПО и воздействия на пользователей;
- оценивать вероятностные и временные характеристики реализации атак вредоносного ПО и воздействия на пользователей социальных сетей;

владеть:

- навыками построения математических моделей осуществления атак на социальных сетей и воздействий на пользователей;
- методикой анализа рисков при реализации атак вредоносного ПО и воздействий на пользователей социальных сетей.

Аннотация программы учебной дисциплины С3.В.ДВ.1.1 «Управление рисками в распределенных информационных системах»

Трудоемкость 14 ЗЕТ (504 часа)

1. Цели и задачи дисциплины

Целью изучения дисциплины является изучение основных этапов процесса управления рисками распределенных информационных систем

(РИС); знакомство с методами принятия решений (экспертных оценок, многокритериального принятия решений при определенности и при неопределенности, обусловленной как случайными воздействиями внешней среды, так и действиями злоумышленника), направленных на снижение риска информационной безопасности.

Задачи дисциплины:

- изучение основных понятий и методов управления рисками информационной безопасности;
- знакомство с менеджментом риска информационной безопасности, включая основные этапы: установление контекста, оценку, обработку, принятие и коммуникацию риска, а также мониторинг и переоценку риска информационной безопасности;
- знакомство с современными стандартами в области управления информационными рисками распределенных информационных систем;
- знакомство с существующими инструментальными средствами для управления рисками;
- изучение методов экспертных оценок, как основного инструмента принятия решений при управлении рисками информационной безопасности РИС в условиях недостаточности объективной информации.

2. Требования к уровню освоения содержания дисциплины

В результате изучения дисциплины студент

должен **знать**:

- основные понятия и методы управления рисками информационной безопасности РИС;
- основные этапы менеджмента риска информационной безопасности РИС;
- современные стандарты в области управления информационными рисками;
- основные понятия и обобщенную классификацию задач принятия решений при управлении рисками информационной безопасности;
- формальное описание моделей принятия решений при управлении рисками информационной безопасности РИС;
- методы экспертных оценок и варианты их использования при управлении рисками информационной безопасности;

уметь:

- организовать систему менеджмента риска информационной безопасности РИС в соответствии со стандартом ГОСТ Р ИСО/МЭК 27001-2006;
- разрабатывать планы обработки рисков информационной безопасности РИС;
- организовать процедуру экспертного оценивания и осуществить обработку экспертной информации;

- формировать множество альтернатив и критерии оптимальности для задач принятия решений при управлении рисками информационной безопасности;

- решать детерминированную многокритериальную задачу выбора мер контроля и управления, направленных на снижение риска информационной безопасности;

- решать многокритериальную задачу выбора мер контроля и управления в условиях неопределенности, обусловленной как случайными воздействиями внешней среды, так и действиями злоумышленника;

- осуществлять постановку оптимизационной задачи выбора защитных мероприятий, направленных на снижение риска информационной безопасности РИС и выбор метода ее решения.

владеть:

- профессиональной терминологией в области менеджмента рисков информационной безопасности РИС;

- методикой менеджмента риска информационной безопасности в соответствии со стандартом ГОСТ Р ИСО/МЭК 27001-2006;

- методикой проведения экспертного оценивания при решении задачи оценки рисков информационной безопасности и управления ими;

- детерминированными методами принятия решений по управлению рисками информационной безопасности (аксиоматическими методами многокритериальной оценки альтернатив, методом аналитической иерархии, методом порогов несравнимости);

- статистическими методами принятия решений по управлению рисками информационной безопасности в условиях неопределенности, обусловленной как случайными воздействиями внешней среды, так и действиями злоумышленника;

- навыками формирования оптимизационных задач, разработки соответствующих оптимизационных моделей и выбора методов их решения.

Программа направлена на реализацию следующих компетенций: ПК-14, ПК-18, ПСК-7.1, ПСК-7.2, ПСК-7.3, ПСК-7.4, ПСК-7.5, ПСК-7.6, ПСК-7.7, ПСК-7.8.

3. Содержание дисциплины, основные разделы

Менеджмент риска информационной безопасности РИС: основные термины и определения; система менеджмента информационной безопасности; менеджмент риска информационной безопасности; стандарты в области управления информационными рисками; инструментальные средства для управления рисками.

Управление рисками РИС: основные понятия и обобщенная классификация задач принятия решений; формальное описание моделей принятия решений; методы экспертных оценок; детерминированные модели и методы принятия решений; статистические модели и методы принятия решений в условиях неопределенности; методы оптимизации.

Аннотация программы дисциплины
С3.В.ДВ.1 «Безопасность распределенных информационных систем государственного и муниципального управления»

Трудоемкость 14 ЗЕТ (504 часа)

Цель и задачи изучения дисциплины

Основная цель состоит в изучении проблем обеспечения ИБ распределенных информационных систем государственного и муниципального управления Российской Федерации.

Основные дидактические единицы (разделы)

Основы государственного и муниципального управления, его информационных технологий и систем. Структура и функции информационных систем государственного и муниципального управления (ИТС ГМУ). Угрозы и принципы построения защищенных информационных технологий и систем государственного и муниципального управления. Оценка и регулирование рисков нарушения безопасности ИТС ГМУ.

Компетенции, приобретаемые студентом в процессе изучения дисциплины ПК-14 ПК-27, ПСК-7.8

В результате изучения дисциплины студенты должны:

знать: основы государственного и муниципального информационного управления в РФ; структуру и функциональную обеспеченность информационных технологий и систем государственного и муниципального управления

уметь: выявлять информационные угрозы в государственных и муниципальных информационных системах; применять средства защиты информационных технологий государственного и муниципального управления

владеть: методологией оценки и регулирования рисков в работе информационных систем и технологий государственного и муниципального управления.

Аннотация программы дисциплины
С3.В.ДВ.1 «Оценка эффективности регионального информационного противоборства»

Трудоемкость 14 ЗЕТ (504 часа)

Цель и задачи изучаемой дисциплины

Основная цель состоит в изучении методического обеспечения

контроля состояния безопасности информации и эффективности ее защиты в ходе противоборства.

Основные дидактические единицы (разделы)

Понятие информационного противоборства. Организация комплексной защиты. Контроль эффективности информационного противоборства. Критерии эффективности регионального информационного противоборства. Меры и средства защиты. Анализ состояния разработок в сфере оценок эффективности средств защиты. Анализ возможных сценариев атаки и постановка задачи оценки эффективности наборов средств защиты. Алгоритм оценки эффективности системы обеспечения безопасности. Комплексная оценка состояния безопасности информации и эффективности противодействия угрозам.

Компетенции, приобретаемые студентом в процессе изучения дисциплины: ПК-12 ПК-16 ПК-33 ПСК-7.3

В результате изучения дисциплины студенты должны:

знать: методы и алгоритмы эффективности информационного противоборства, включая контроль на уровне региональных систем управления защитой информации; информации.

уметь: выявлять факторы и тенденции в области обеспечения безопасности информации; аналитически оценивать эффективность информационного противоборства угрозам;

владеть: методиками построения и оценки эффективности защиты информационных систем от внутренних и внешних угроз.

Аннотация программы дисциплины С4 «Физическая культура»

Трудоемкость 2 ЗЕТ (396 часов)

Цели и задачи изучения дисциплины

целью физического воспитания является содействие подготовке гармонично развитых, высококвалифицированных специалистов.

Для достижения цели ставятся задачи:

воспитание у студентов высоких моральных, волевых и физических качеств, готовности к высокопроизводительному труду; сохранение и укрепление здоровья студентов, содействие правильному формированию и всестороннему развитию организма, поддержание высокой работоспособности на протяжении всего периода обучения; всесторонняя физическая подготовка студентов; профессионально - прикладная физическая подготовка студентов с учётом особенностей их будущей трудовой деятельности; приобретение студентами необходимых знаний по основам теории, методики и организации физического воспитания и спортивной тренировки, подготовка к работе в качестве общественных инструкторов, тренеров и судей; совершенствования спортивного мастерства студентов - спортсменов; воспитание у студентов убеждённости в необходимости регулярно заниматься физической культурой и спортом.

Основные дидактические единицы (разделы)

Физическая культура в общекультурной и профессиональной подготовке студентов; ее социально-биологические основы; физическая культура и спорт как социальные феномены общества; законодательство Российской Федерации о физической культуре и спорте; физическая культура личности; основы здорового образа жизни студента; особенности использования средств физической культуры для оптимизации работоспособности; общая физическая и специальная подготовка в системе физического воспитания; спорт; индивидуальный выбор видов спорта или систем физических упражнений; профессионально-прикладная физическая подготовка студентов; основы методики самостоятельных занятий и самоконтроль за состоянием своего организма.

Компетенции, приобретаемые студентом в процессе изучения дисциплины ОК-12

В результате изучения дисциплины студент должен:

знать: основные понятия и термины, закономерности, теории, принципы и положения, раскрывающие сущность явлений в физической культуре; объективные связи между ними;

уметь: адаптивно, творчески использовать полученные специальные знания на занятиях по физическому воспитанию для личностного и профессионального развития, самосовершенствования, организации здорового стиля жизни при выполнении учебной, профессиональной и социокультурной деятельности;

владеть: системой научно-практических и специальных знаний, необходимых для понимания природных и социальных процессов функционирования физической культуры общества и личности; навыками предметно-операционального использования полученных знаний и приобретения практического опыта в занятиях избранным видом спорта или системой физических упражнений.

Виды учебной работы: практические занятия.

Изучение дисциплины заканчивается зачетом.

Аннотация программы учебной практики (С5.У)

Трудоемкость 3 ЗЕТ (108 часов)

1. Цель задачи практики

Учебная практика является составной частью учебного процесса подготовки квалифицированных специалистов. Во время практики происходит закрепление и конкретизация результатов теоретического обучения, приобретение студентами умения и навыков практической работы по избранной специальности и присваиваемой квалификации.

Цель практики - развитие навыков познавательной деятельности, ведения самостоятельной работы по поиску и анализу информации, формирование способности понимать и анализировать деятельность

специалиста по безопасности распределенных информационных систем, овладение методикой исследования, экспериментирования и оформления документации; сбор материалов для курсового и дипломного проектирования.

Задачами практики являются:

- Познакомиться со спецификой основных методов обеспечения информационной безопасности и требованиями к ним;
- Познакомиться с видами и задачами работы специалиста по безопасности распределенных компьютерных систем: проанализировать и определить место и значение каждого вида деятельности (научно-исследовательская; проектно - конструкторская; контрольно- аналитическая; организационно-управленческая; эксплуатационная).

Для успешного прохождения учебной практики необходимо освоение дисциплин «Социотехнические основы ИБ», «Основы национальной безопасности», «Информационно-психологическая безопасность». Прохождение учебной практики необходимо для дальнейшего освоения дисциплин «Управление информационной безопасностью», «Информационные операции и атаки в распределенных информационных системах», «Управление рисками в РИС», прохождения производственной и преддипломной практики.

Общее методическое руководство практикой и непосредственное руководство осуществляет преподаватель, утвержденный приказом ректора или проректора по учебной работе.

Руководство практикой студентов в структурном подразделении – базе практики – возлагается на специалистов указанных подразделений. Руководитель практики от организации осуществляет повседневное организационно-методическое руководство и контроль хода практики закрепленного за ним студента и определяет ему конкретное задание, помогает в сборе необходимых материалов.

Основными нормативно-методическими документами, регламентирующими работу студентов на практике, являются программа практики, а также методические указания руководителя практики от ВГТУ.

По окончанию практики необходимо представить не позднее последнего дня практики отчет по практике. Отчет представляется на кафедру.

2. Требования к уровню освоения практики

В результате прохождения практики студент должен :

- знать:

- виды и задачи работы специалиста по безопасности распределенных компьютерных систем на конкретном предприятия (места практики);
- место и значение каждого вида деятельности (научно-исследовательская;проектно-конструкторская;контрольно-аналитическая;организационно-управленческая;эксплуатационная) в деятельности специалиста по информационной безопасности в конкретной организации.

- уметь:

- выявлять естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности, и применять соответствующий физико-математический аппарат для их формализации, анализа и выработки решения;
- применять математический аппарат, в том числе с использованием вычислительной техники, для решения профессиональных задач;
- использовать нормативные правовые документы в своей профессиональной деятельности;

- владеть:

- методикой исследования с использованием компьютерных технологий;
- методикой анализ защищенности автоматизированных систем.

3. Содержание ознакомительной практики

3.1Техника безопасности, противопожарные меры.
3.2Подготовка задач исследования.
3.3Работа на ПК.
3.4Перифирийные устройства. Аппаратный интерфейс.
3.5Порядок обслуживания компонентов компьютера и периферийных устройств.
3.6Знакомство с сетевым администрированием.
3.7Знакомство с организацией защиты информации на предприятии.
3.8Состав и структура системы защиты предприятия.
3.9Порядок обслуживания средств защиты информации.

4. Индивидуальные задания

Программа направлена на реализацию следующих компетенций:
ОК-1; ОК-11; ПК-1

Аннотация программы производственной практики (С5.У)

Трудоемкость 6 ЗЕТ (216 часов)

1. Целью практики является приобретение и совершенствование практических навыков в выполнении обязанностей по должностному предназначению, углубления и закрепления полученных знаний, умений и навыков.

Задачами практики являются:

- повышение уровня теоретических и практических знаний по обеспечению безопасности распределенных компьютерных систем;
- ознакомление с организацией работы службы обеспечения безопасности распределенных компьютерных систем конкретного предприятия.

2. Требования к уровню освоения практики

В результате прохождения практики студент должен :

- знать

как на предприятии (место практики) выполнятся работы

а) контрольно-аналитической деятельности: - контроль работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации;

- экспериментально-исследовательские работы при сертификации средств защиты автоматизированных систем;

- Экспериментально-исследовательские работы при аттестации автоматизированных систем;

- инструментальный мониторинг защищенности автоматизированных систем;

б) организационно-управленческой деятельности:

- организация работы коллектива, принятие управленческих решений, определение порядка выполнения работ;

- разработка предложений по совершенствованию и повышению эффективности принятых мер по обеспечению безопасности распределенных компьютерных систем;

- организация работ по выполнению требований защиты информации ограниченного доступа;

- методическое и организационное обеспечение безопасности распределенных компьютерных систем;

- организация работ по созданию, внедрению, эксплуатации и сопровождению защищенных распределенных компьютерных систем;

- контроль реализации политики информационной безопасности;

в) эксплуатационной деятельности:

- реализация информационных технологий в сфере профессиональной деятельности с использованием защищенных распределенных компьютерных систем;

- администрирование подсистем безопасности распределенных компьютерных систем;

- мониторинг безопасности распределенных компьютерных систем;

- управление безопасности распределенных компьютерных систем;

- обеспечение восстановления работоспособности систем защиты информации при возникновении нештатных ситуаций.

- уметь:

- выполнять некторые виды указанных выше работ

- владеть:

- методикой выполнения указанных выше работ.

3. Содержание практики

Производственная практика ориентирована на ознакомление и приобретение навыков в одном (или нескольких взаимосвязанных) из ниже перечисленных вопросов.

Изучение организационного строения базовых предприятий (организаций), назначения отдельных подразделений и служб, а также их взаимодействия.

Изучение используемых в структуре предприятия методов обработки исходных материалов и соответствующих средств, а также оборудования, предназначенного для этих целей.

Приобретение практических навыков по разработке и (или) подготовке конструкторско-технологической документации для производства аппаратуры защиты информации с учетом традиционных для базового предприятия исходных материалов, оборудования и методов обработки.

Изучение принципов работы и приобретение навыков практического использования оборудования для автоматизированной подготовки конструкторско-технологической документации при подготовке производства к серийному выпуску изделий.

Ознакомление с методами и соответствующим оборудованием для производства и контроля годности аппаратуры. Приобретение практических навыков работы с оборудованием для контроля и локализации технологических дефектов после автоматизированной сборки модулей средств защиты информации.

Изучение методов технико-экономического обоснования и технологической подготовки производства при выпуске новых изделий.

Изучение структуры, состава программно-аппаратных средств защиты информации и информационных систем.

Изучение и практическое применение новых информационных технологий для решения разнообразных прикладных задач и разработки специализированных комплексов защиты информации.

Патентно-информационное исследование по выбору вариантов возможных решений по теме и их оценке, сопоставление с техническим уровнем современных отечественных и зарубежных аналогов.

Разработка и оформление рабочих чертежей и другой технической и эксплуатационной документации на спроектированное изделие или программные средства.

Разработка и применение машинных методов проектирования изделий, разработки чертежей и технологических процессов.

Анализ технологического процесса как объекта управления, модели объекта и законы управления.

Техническое проектирование средств защиты информации.

Разработка отдельных подсистем защиты информации.

Разработка рабочей документации.

Определение эффективности разработанных методов и качества составленных программ.

Программа направлена на реализацию следующих компетенций: ОК-1; ОК-11; ПК-1; ПК-40

Аннотация программы преддипломной практики (С5.П)

Трудоемкость 6 ЗЕТ (216 часов)

ЦЕЛЬ ПРАКТИКИ

Овладение навыками самостоятельного выполнения работы по будущей специальности, сбор фактического материала по теме дипломного проекта (работы).

ЗАДАЧИ ПРАКТИКИ

Закрепление и углубление знаний, полученных студентами в процессе обучения в ВГТУ, на основе глубокого изучения работы предприятия, на котором работают и проходят практику студенты.

В производственных условиях конкретного предприятия студенты более подробно изучают технологию производства, экономику, организацию и управление производством, стандартизацию и контроль качества продукции, оборудование, радиоаппаратуру, вычислительную технику, средства и системы защиты информации, контрольно-измерительные приборы, а также механизацию и автоматизацию производственных процессов, передовой опыт работы, организацию научно-исследовательской, проектно-конструкторской, рационализаторской и изобретательской работы.

СОДЕРЖАНИЕ ПРЕДДИПЛОМНОЙ ПРАКТИКИ

3.1. Практическое ознакомление с порядком проектирования средств защиты информации на базе современных средств, схемотехнического моделирования, разработка технического задания.

3.2. Патентно-информационный поиск по тематике выпускной квалификационной работы.

3.3. Сбор фактического материала, необходимого для принятия правильного решения при выборе принципа работы схемы и конструкции проектируемого средства защиты информации.

3.4. Определение вопросов, требующих проработки научно - исследовательского характера, разработка методики и плана этих исследований, предполагая их реализацию в процессе дипломного проектирования.

3.5. Сбор фактического материала по вопросам организации и планирования процесса проектирования изделия: разработка организационно-экономических вопросов, связанных с тематикой дипломного проектирования.

3.6. Конкретное содержание преддипломной практики определяется тематикой дипломного проекта (работы), выполняемого студентом.

Программа направлена на реализацию следующих компетенций: ОК-1; ОК-11; ПК-1; ПК-40

Итоговая государственная аттестация

Итоговая государственная аттестация включает государственный междисциплинарный экзамен и защиту выпускной квалификационной работы (дипломной работы).

Государственный междисциплинарный экзамен

1. Требования к программе комплексного экзамена:

1.1 В программе должны быть представлены разделы по трем направлениям:
математика (математический анализ, алгебра, теория вероятностей и математическая статистика, структуры данных и алгоритмы); защита информации (теория информации; физические основы защиты информации; криптографические методы защиты информации, техническая защита информации, организационное и правовое обеспечение информационной безопасности и др.). Специализация (информационная безопасность распределены информационных систем; технология построения защищенных распределенных приложений; управление рисками в распределенных информационных системах).

1.2 Общее количество вопросов программы – не более 100.

1.3. Каждый билет содержит 3 вопроса.

1.4. В качестве вопросов должны формулироваться основные теоретические положения, предполагающие их развернутое обоснование при ответе.

1.5. Формулировка каждого вопроса должна четко определять рамки и объем содержания ответа.

2. Содержание дисциплины, основные разделы

I. МАТЕМАТИКА

Раздел 1. Математический анализ

Раздел 2. Теория вероятности и математическая статистика

Раздел 3. Алгебра

Раздел 4. Структуры данных и алгоритмы (алгоритмы на графах).

II. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Раздел 1. Теория информации

Раздел 2. Защита информации

Раздел 3. Безопасность операционных систем, баз данных и вычислительных сетей.

Раздел 4. Организационное и правовое обеспечение информационной безопасности.

III. Специальные дисциплины.

Выпускная квалификационная работа

Выпускная квалификационная работа (ВКР) является заключительным этапом обучения и выполняется с целью практического применения полученных знаний и навыков при решении инженерных задач обеспечения информационной безопасности систем.

Выпускная квалификационная работа состоит из расчетно-пояснительной записки ВКР с иллюстративным графическим материалом, размещенным по разделам работы, отзыва руководителя и рецензии, а также (по необходимости) документов, подтверждающих апробацию, публикацию и внедрение результатов работы.

В результате выполнения ВКР выпускник должен продемонстрировать:

- **знание** риск-образующих факторов и угроз деструктивного нарушения информационной безопасности в компьютерных системах;

- **умение** осуществлять рациональный выбор средств и применять известные методы риск-анализа процессов нарушения информационной безопасности в распределенных компьютерных системах; на основе оценки величины и частоты возможных ущербов строить риск-модели компьютерных систем;

- **владение** методологией управления информационными рисками и прогнозирования эффективности защиты распределенных компьютерных систем, подвергающихся воздействию угроз нарушения информационной безопасности.