

Аннотация к рабочей программе

дисциплины «Физика»

по направлению 090900.62 Информационная безопасность

(профиль «Безопасность автоматизированных систем»).

Общая трудоемкость дисциплины составляет 8 зачетных единиц.

Форма контроля: экзамен, экзамен.

Семестры: 2, 3.

Целями освоения учебной дисциплины (модуля) являются формирование у студента знаний и навыков научного мировоззрения и современного физического мышления. Курс физики совместно с курсами физико-математического цикла составляет основу теоретической подготовки и играет роль фундаментальной физико-математической базы, без которой невозможна успешная деятельность бакалавра любого профиля.

Задачами курса являются: формирование целостного представления, умений и навыков: по теоретическим и практическим проблемам в изучении основных законов классической и современной физики, а также освоении методов физического исследования; формирование навыков самостоятельного, творческого использования теоретических и практических знаний при решении конкретных задач; формирование навыков работы с современной научной аппаратурой; формирование навыков проведения физического эксперимента; применение полученных навыков и умений в профессиональной деятельности.

Учебная дисциплина «Физика» входит в математический и естественнонаучный цикл (базовая часть) и относится к числу фундаментальных дисциплин, поскольку служит основой для изучения учебных дисциплин как математического и естественнонаучного, так и профессионального цикла.

Знания, полученные по дисциплине «Физика», непосредственно используются при изучении дисциплин базового цикла:

- «Математика»;
- «Информатика»;
- «Теория информации»;
- «Теория вероятностей и математическая статистика»;
- «Дискретная математика».

и дисциплин профессионального цикла:

- «Основы информационной безопасности»;
- «Аппаратные средства вычислительной техники»;
- «Программно-аппаратные средства защиты информации»;
- «Криптографические методы защиты информации»;
- «Техническая защита информации»;
- «Организационное и правовое обеспечение информационной безопасности»;
- «Сети и системы передачи информации»;
- «Безопасность жизнедеятельности»;
- «Языки программирования»;

- «Технология и методы программирования»;
- «Управление информационной безопасностью»;
- «Документоведение»;
- «Электротехника»;
- «Электротехника и схемотехника»;

Краткое содержание дисциплины:

Физические основы механики. Элементы кинематики. Динамика частиц. Система материальных точек. Законы сохранения энергии, импульса, момента импульса. Элементы механики сплошных сред

Основы молекулярно-кинетической теории. Микроскопическое состояние вещества. Статистические распределения. Основы термодинамики. Явления переноса.

Электростатика. Постоянный электрический ток. Электрический ток в металлах и вакууме.

Магнитное поле. Электромагнитная индукция. Магнитные свойства вещества. Основы теории Максвелла.

Механические и электромагнитные колебания. Электромагнитные волны.

Элементы геометрической и электронной оптики. Элементы фотометрии. Волновая оптика.

Квантовая природа излучения. Экспериментальное обоснование идей квантовой теории. Квантовое состояние. Уравнение Шредингера.

Атом. Модели атома. Атомное ядро.

Основы физики твердого тела.

Элементы физики элементарных частиц.

Современная физическая картина мира.

В результате изучения дисциплины бакалавр должен обладать следующими общекультурными и профессиональными компетенциями:

ОК-9: способностью логически верно, аргументированно и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии;

ОК-12: способностью критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков;

ПК-1: способностью использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности;

ПК-2: способностью 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;

ПК-18: способностью собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности;

ПК-19: способностью составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности;

ПК-20: способностью применять методы анализа изучаемых явлений, процессов и

проектных решений;

ПК-22: способностью проводить эксперименты по заданной методике, обработку результатов, оценку погрешности и достоверности их результатов;

ПК-23: способностью принимать участие в проведении экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности;

ПК-24: способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности;

Аннотация к рабочей программе по дисциплине БЗ.ДВ.3 «Интегрированные информационные системы в управлении»

**Направление подготовки 090900.62 «Информационная безопасность»
(Профиль «Безопасность автоматизированных систем»)**

Общая трудоёмкость дисциплины составляет 144/4 час./ зачетных единиц.

Предполагаемые семестры: 8.

Форма контроля: экзамен 8 семестр

Целями освоения учебной дисциплины являются: получение студентами комплекса знаний в области способов и методов проектирования, моделирования, настройки на объект управления и развития интегрированных систем в управлении, опирающиеся на общую методологию проектирования информационных систем, методы формального и инженерного конструирования и математическое, информационное и программное обеспечение современных ERP-систем, содействовать формированию системного мышления.

Задачами дисциплины являются: формирование целостного представления о принципах построения, структуры и функциональных возможностях современных интегрированных систем в управлении, составе и структуры бизнес-процессов на предприятии, стандартах построения интегрированных информационных систем – MRP, MRP II, ERP, ERP II, языковой среде и методах настройки и развития современных ERP – систем.

Учебная дисциплина «Интегрированные информационные системы в управлении» относится к циклу СЗ. Для освоения дисциплины необходимы знания, полученные при изучении следующих дисциплин:

- «Организация ЭВМ и вычислительных сетей»;
- «Информационные системы»;

- «Технологии и методы программирования»;
- «Системы управления базами данных».

В дисциплине «Интегрированные информационные системы в управлении» определяются теоретические основы и практические навыки, при освоении которых студент получает знания, необходимые инженеру в производственной деятельности;

Краткое содержание дисциплины:

Архитектура ERP-систем. Бизнес-процессы и стандарты.

Динамическое моделирование предприятия.

Производство. Планирование.

Склады и управление заказами.

Финансы. Сервис.

Управление жизненным циклом продукта.

Анализ финансово-хозяйственного состояния предприятия.

В результате изучения дисциплины бакалавр должен обладать следующими профессиональными компетенциями (ПК):

общекультурными компетенциями (ОК):

способностью к кооперации с коллегами, работе в коллективе (ОК-5);

способностью находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность (ОК-6);

способностью осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности, готовностью и способностью к активной созидательной деятельности в условиях информационного противоборства (ОК-7);

способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления (ОК-8);

способностью логически верно, аргументированно и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии (ОК-9);

профессиональными компетенциями (ПК)

способностью формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности (ПК-4);

способностью организовывать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации (ПК-5);

способностью организовать проведение и сопровождать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов (ПК-6);

способностью использовать основные методы защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий (ПК-7);

способностью 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 (ПК-

8);

способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью (ПК-25);

способностью формировать комплекс мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью (ПК-26);

способностью принимать участие в организации контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-27);

способностью изучать и обобщать опыт работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации (ПК-28);

способностью участвовать в работах по реализации политики информационной безопасности (ПК-29);

способностью применять комплексный подход к обеспечению информационной безопасности в различных сферах деятельности (ПК-30);

способностью организовать работу малого коллектива исполнителей с учетом требований защиты информации (ПК-31);

способностью организовать мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств защиты информации (ПК-32);

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-33).

**Аннотация к рабочей программе
дисциплины «Противодействие техническим разведкам»
по направлению подготовки 090900.62 «Информационная безопасность»
(Профиль «Безопасность автоматизированных систем»)**

Общая трудоемкость дисциплины составляет 3 зачетных единиц

Форма контроля: зачет

Предполагаемые семестры: 6

Цель курса «Противодействие техническим разведкам» приобрести теоретические знания и навыки работы, необходимые для защиты информационных ресурсов организации от приемов конкурентов, направленных на изъятие с помощью технических средств интересующих сведений, искажения или стирания хранимой информации.

Задачи курса:

В результате изучения дисциплины бакалавр должен:

Знать:

- технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации;

- принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации.

Уметь:

- осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты;

- анализировать и оценивать угрозы информационной безопасности объекта.

Владеть:

- методами и средствами выявления угроз безопасности АС;

- методами технической защиты информации.

Учебная дисциплина «Противодействие техническим разведкам» входит в профессиональный цикл дисциплина по выбору БЗ.ДВ.7

Знания, полученные по дисциплине, непосредственно используются студентами при разработке курсовых и дипломных работ, в научно-исследовательской работе и для изучения следующих базовых дисциплин:

- технология построения защищенных автоматизированных систем;
- комплексное обеспечение информационной безопасности автоматизированных систем;
- интегрированные информационные системы в управлении.

Краткое содержание дисциплины

Механизмы и технологии технической разведки. Системный подход к формированию общих принципов и основных способов противодействия техническим разведкам. Скрытие демаскирующих признаков. Противодействие радио и радиотехнической разведке. Физические и технические основы противодействия видовой разведке. Технический контроль защиты объектов от утечки информации за счет побочных электромагнитных излучений. Организация службы безопасности; функции, задачи и направления деятельности.

В результате изучения дисциплины бакалавр должен обладать следующими профессиональными компетенциями:

ОК-1: способностью осознавать необходимость соблюдения Конституции Российской Федерации, прав и обязанностей гражданина своей страны, гражданского долга и проявления патриотизма.

ОК-2: способностью осуществлять свою деятельность в различных сферах общественной жизни с учетом принятых в обществе моральных и правовых норм.

ОК-3: способностью уважительно и бережно относиться к историческому наследию и культурным традициям, толерантно воспринимать социальные и культурные различия.

ОК-8: способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления.

ОК-12: способностью критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков.

ПК-2: способностью проводить анализ защищенности автоматизированных систем.

**Аннотация к рабочей программе
дисциплины «Вычислительная математика»
по направлению 090900.62 Информационная безопасность
(профиль «Безопасность автоматизированных систем»).**

Общая трудоемкость дисциплины составляет 5 зачетных единиц.

Форма контроля: экзамен.

Предполагаемые семестры: 3.

Целями освоения учебной дисциплины являются: воспитание математической культуры, развитие навыков математического, алгоритмического мышления и программирования, обучение применению и программной реализации вычислительных методов.

Задачами курса являются:

- знакомство с реально используемыми в вычислительной практике алгоритмами,
- изучение особенностей численных методов для решения инженерных задач,
- программная реализация изученных методов,
- оценка погрешности полученного решения.

Курс «Вычислительная математика» является математическим курсом, в системе подготовки специалиста по информационной безопасности. Этот курс должен научить студента, если не удастся решить задачу аналитически, решать ее численным методом.

Для успешного усвоения дисциплины необходимо, чтобы студент владел знаниями, умениями, навыками, полученными в процессе изучения курсов:

«Математический анализ»

«Алгебра»

«Языки программирования»

«Вычислительная математика» используется при изучении следующих дисциплин:

«Технологии и методы программирования»

«Информационно-аналитическая работа по обеспечению информационной безопасностью АС»

«Основы прогнозирования».

Краткое содержание дисциплины:

Основные сведения из теории погрешностей

Итерационные методы решения СЛАУ

Решение нелинейных уравнений и систем

Методы приближения и аппроксимации функций.

Численное дифференцирование и численное интегрирование

Приближенное интегрирование обыкновенных дифференциальных уравнений

Математические программные системы

В результате изучения дисциплины бакалавр должен обладать следующими общекультурными и профессиональными компетенциями:

ОК-8: Способность к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления.

ОК-9: Способность логически верно, аргументировано и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии.

ОК- 11: Способностью к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства.

ОК- 12: Способность критически оценивать свои достоинства и недостатки.

ПК-1: Способность использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности.

Аннотация к рабочей программе дисциплины «Криптографические методы защиты информации» по направлению 090909.62 Информационная безопасность (профиль «Безопасность АС»).

Общая трудоемкость дисциплины составляет 4 зачетные единицы.

Форма контроля: экзамен

Предполагаемые семестры: 6

Основной целью дисциплины «Криптографические методы защиты информации» является изложение основополагающих принципов защиты информации с помощью криптографических методов и примеров реализации этих методов на практике.

Задачи дисциплины «Криптографические методы защиты информации» - дать основы:

- системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения криптографических методов;
- принципов разработки шифров;
- математических методов, используемых в криптографии.

Учебная дисциплина относится к циклу БЗ. Изучение дисциплины «Криптографические методы защиты информации» базируется на дисциплинах: «Математика», «Дискретная математика», «Теория вероятностей и математическая статистика», «Теория информации», «Математическая логика и теория алгоритмов».

Дисциплина «Криптографические методы защиты информации» обеспечивает изучение дисциплин:

- «Разработка и эксплуатация защищенных автоматизированных систем»;
- «Управление информационной безопасностью»;
- «Информационная безопасность автоматизированных транспортных систем»;
- «Защита электронного технологического документооборота»;
- «Информационная безопасность информационно-управляющих и информационно-логистических систем транспорта»;
- «Организация работы администратора автоматизированных систем»;
- Основы информационного противоборства и др.

Знания и практические навыки, полученные из дисциплины «Криптографические методы защиты информации», используются обучаемыми при разработке курсовых и дипломных работ, в научно-исследовательской работе.

Краткое содержание дисциплины:

Исторический обзор. Открытые сообщения и их характеристики

Основные задачи и понятия криптографии. Перечень угроз. Симметричное и асимметричное шифрование в задачах защиты информации. Шифры с открытым ключом

и их использование. Классификация шифров. Модели шифров. Основные требования к шифрам. Простейшие криптографические протоколы. Разновидности шифров перестановки: маршрутные и геометрические перестановки. Элементы криптоанализа шифров перестановки. Поточные шифры замены. Шифры простой замены и их анализ. Многоалфавитные шифры замены. Шифры гаммирования и их анализ. Использование неравновероятной гаммы, повторное использование гаммы, криптоанализ шифра Виженера. Тесты У.Фридмана. Блочные шифры простой замены и особенности их анализа. Современные блочные шифры. Криптоалгоритм DES. Криптоалгоритм ГОСТ-28147-89. Криптоалгоритм AES. Надёжность шифров. Методы синтеза и анализа симметричных шифрсистем. Хеш-функции и их криптографические приложения.

В результате изучения дисциплины специалист должен обладать следующими профессиональными компетенциями:

общекультурными (ОК):

ОК-7: способностью осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности, готов и способностью к активной состязательной деятельности в условиях информационного противоборства;

профессиональными (ПК):

общепрофессиональными:

ПК-1: способностью использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности;

ПК-4: способностью формировать комплекс мер по информационной безопасности с учетом 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 учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации;

ПК-11: способностью выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации;

проектно-технологическая деятельность:

ПК-15: способностью применять программные средства системного, прикладного и специального назначения;

ПК-21: способностью проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов;

ПК-24: способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам

обеспечения информационной безопасности;

организационно-управленческая деятельность:

ПК-27: способностью принимать участие в организации контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации;

ПК-28: способностью изучать и обобщать опыт работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации.

**Аннотация к рабочей программе
дисциплины «Математическая логика и теория алгоритмов»
по направлению 090900.62 Информационная безопасность
(профиль «Безопасность автоматизированных систем»).**

Общая трудоемкость дисциплины составляет 4 зачетных единицы.

Форма контроля: экзамен.

Предполагаемые семестры: 4.

Целями освоения учебной дисциплины являются: развитие способности студентов к строгому абстрактно-формальному логическому и алгоритмическому мышлению, получение практических навыков решения задач и построения доказательств.

Задачами курса являются:

- освоение теории множеств, понимание принципов аксиоматического метода, синтаксиса и семантики,
- накопление опыта работы с формализованными языками, пропозициональными и предикатными исчислениями,
- изучение формулировок и доказательств основных теорем курса,
- усвоение основ теории алгоритмов, необходимых для доказательства фундаментальных теорем Геделя о неполноте и неразрешимости арифметики.

Вопросы, изучаемые в курсе математической логики и теории алгоритмов, базируются на общематематических курсах, изучаемых студентами на предыдущих семестрах, в частности, в курсах математического анализа, вычислительной и дискретной математики.

Краткое содержание дисциплины:

Теория булевых функций
Логика высказываний
Функции алгебры логики
Приложения алгебры логики
Логика предикатов
Исчисление высказываний
Исчисление предикатов
Проблемы полноты и разрешимости формальных систем
Формализация понятия алгоритма. Рекурсивные функции
Машины Поста, Тьюринга

Нормальные алгоритмы Маркова

Проблемы алгоритмической неразрешимости и сложности алгоритмов

В результате изучения дисциплины бакалавр должен обладать следующими общекультурными и профессиональными компетенциями:

способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления (ОК-8);

способностью логически верно, аргументировано и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии (ОК-9);

способностью к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства (ОК-11);

способностью критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков (ОК-12);

способностью использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности (ПК-1).

**Аннотация к рабочей программе
дисциплины «Основы информационной безопасности»
по направлению подготовки 090900.62 «Информационная безопасность»
(Профиль «Безопасность автоматизированных систем»)**

Общая трудоемкость дисциплины составляет 3 зачетные единицы

Форма контроля: зачет

Предполагаемые семестры: 1

Цель освоения дисциплины «Основы информационной безопасности»:

- сформировать у студентов знания по основам обеспечения информационной безопасности в различных областях деятельности современного общества.

Задачами курса являются:

- дать студентам необходимые знания, умения и навыки, в том числе:
- теоретические и практические проблемы обеспечения информационной безопасности на предприятиях, транспорте и в бизнесе;
- навыки самостоятельного, творческого использования теоретических знаний для предотвращения незаконного использования информации в практической деятельности.

Учебная дисциплина «Основы информационной безопасности» входит в профессиональный цикл (базовая часть).

Знания, полученные по дисциплине, непосредственно используются студентами при разработке курсовых и дипломных работ, в научно-исследовательской работе и для изучения следующих базовых дисциплин:

- теория принятия решений;
- программно-аппаратные средства защиты информации;
- управление информационной безопасностью;
- технология построения защищенных автоматизированных систем;
- информационная безопасность открытых систем;
- технология защиты информации.

Краткое содержание дисциплины

Информационная безопасность (ИБ) в системе национальной безопасности Российской Федерации. Виды безопасности. Общеметодологические принципы теории ИБ. Основные понятия. Анализ угроз ИБ, проблемы информационной войны.

Законодательный уровень информационной безопасности. Российское и зарубежное законодательство в области ИБ. Государственная информационная политика. Проблема региональной ИБ. Причины, виды и каналы утечки и искажения информации. Методы и способы обнаружения утечки информации. Функции и механизмы информационной безопасности.

В результате изучения дисциплины бакалавр должен обладать следующими профессиональными компетенциями:

ОК-1: способностью осознавать необходимость соблюдения Конституции Российской Федерации, прав и обязанностей гражданина своей страны, гражданского долга и проявления патриотизма.

ОК-7: способностью осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности, готовностью и способностью к активной созидательной деятельности в условиях информационного противоборства.

ОК-11: способностью к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства.

ПК-3: способностью использовать нормативные правовые документы в своей профессиональной деятельности.

ПК-8: способностью 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.

ПК-18: способностью собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности.

ПК-19: способностью составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности.

ПК-20: способностью применять методы анализа изучаемых явлений, процессов и проектных решений.

ПК-24: способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности.

ПК-29: способностью участвовать в работах по реализации политики информационной безопасности.

ПК-30: способностью применять комплексный подход к обеспечению информационной безопасности в различных сферах 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.

Аннотация к рабочей программе

дисциплины «Управление информационной безопасностью»

направление 090900.62 Информационная безопасность (профиль «Безопасность АС»)

Общая трудоемкость дисциплины составляет 3 зачетные единицы.

Форма контроля: Зачет.

Предполагаемые семестры: 5.

Цели освоения дисциплины «Управление информационной безопасностью» состоят:

- в изучении способов управления информационной безопасностью в организациях, государственных учреждений и на предприятиях, эксплуатирующих АС;
- в решении задач, требующих классификации и структуризации объектов информационной безопасности от степени конфиденциальности.

Задачами курса являются: изучение основных нормативных, правовых актов в области обеспечения ИБ и нормативных методических документов ФСБ России и ФСТЭК России в области защиты информации; изучение моделей нарушителя в АС; разрабатывать модели угроз и нарушителей ИБ АС; выявлять уязвимости информационно-технологических ресурсов автоматизированных систем, проводить мониторинг угроз безопасности автоматизированных систем; оценивать информационные риски в автоматизированных системах; составлять аналитические обзоры по вопросам обеспечения информационной безопасности автоматизированных систем.

Дисциплина *«Управление информационной безопасностью»* относится к циклу БЗ.Б.13. Для освоения дисциплины необходимы знания, полученные при изучении следующих дисциплин:

- основы информационной безопасности;
- программно-аппаратные средства обеспечения информационной безопасности;
- криптографические методы защиты информации.

В дисциплине «Управление информационной безопасностью» определяются теоретические основы и практические навыки, при освоении которых студент способен приступить к изучению следующих дисциплин в соответствии с учебным планом:

- информационная безопасность автоматизированных транспортных систем;
- информационная безопасность информационно-управляющих и информационно-логистических систем.

Краткое содержание дисциплины:

Нормативно-правовая база управления безопасностью.

Методология управления ИБ. Информационная инфраструктура организации.

Политика и программа информационной безопасности в организациях и учреждениях. Оценка и идентификация активов. Анализ угроз и их последствий, выявление уязвимых мест в защите. Управление рисками. Выбор и реализация мер защиты информационных ресурсов. Контроль уровня защищенности.

В результате изучения дисциплины бакалавр должен обладать следующими профессиональными компетенциями:

ОК-5: способностью к кооперации с коллегами, работе в коллективе;

ОК-6: способностью находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность;

ОК-7: способностью осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения ИБ, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства;

ПК-1: способностью использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности;

ПК-2: способностью 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;

ПК-3: способностью использовать нормативные правовые документы в своей профессиональной деятельности.

ПК-4: способностью формировать комплекс мер по информационной безопасности с учетом 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 учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации;

ПК-8: способностью 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.

ПК-9: способностью принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия.

ПК-10: способностью администрировать подсистемы ИБ объекта.

ПК-12: способностью участвовать в разработке подсистемы управления информационной безопасностью.

ПК-15: способностью применять программные средства системного, прикладного и специального назначения.

ПК-16: способностью использовать инструментальные средства и системы программирования для решения профессиональных задач.

ПК-19: способностью составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности.

ПК-21: способностью проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов.

ПК-24: способностью осуществлять подбор, изучение и обобщение научно-

технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности.

ПК-25: способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью.

ПК-26: способностью формировать комплекс мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью.

ПК-29: способностью участвовать в работах по реализации политики информационной безопасности.

ПК-30: способностью применять комплексный подход к обеспечению информационной безопасности в различных сферах деятельности.

ПК-31: способностью организовать работу малого коллектива исполнителей с учетом требований защиты информации.

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.

***Аннотация к рабочей программе
дисциплины «Английский язык в сфере профессиональной
коммуникации (в информатике)»
по направлению 090900.62 Информационная безопасность
(профиль «Безопасность автоматизированных систем»).***

Общая трудоемкость дисциплины составляет 8 зачетных единиц.

Форма контроля: экзамен

Предполагаемые семестры: 1, 2, 3, 4

Целями освоения данной дисциплины являются:

1. Повышение уровня владения иностранным языком, достигнутого в ходе изучения предшествующих дисциплин: «Иностранный язык», «Деловой иностранный язык»;
2. Овладение студентами необходимым и достаточным уровнем коммуникативной иноязычной компетенции для решения социально-коммуникативных задач в области профессиональной и научной деятельности при общении с зарубежными партнерами, а также для дальнейшего самообразования.

Задачами курса являются: повышение уровня учебной автономии, способности к самообразованию; развитие когнитивных и исследовательских умений; развитие информационной культуры; расширение кругозора и повышение общей культуры студентов; воспитание толерантности и уважения к духовным ценностям разных стран и народов.

Учебная дисциплина «Английский язык в сфере профессиональной коммуникации (в информатике)» относится к вариативной части цикла ГСЭ и является гуманитарной и общепрофессиональной основой системы подготовки выпускника технического вуза. Знания, полученные по дисциплине «Иностранный язык в

сфере профессиональной коммуникации» являются инструментом для получения информации о международных стандартах и достижениях в области будущей профессиональной деятельности.

Краткое содержание дисциплины:

Лексика:

- научно-техническая терминология в рамках тем, заявленных в программе:

1. Деловые контакты онлайн;
2. Иностранный язык в профессиональном общении.
3. Трудоустройство. Поиски работы;
4. Научно-техническая литература (профессионально-ориентированная).

Грамматика:

- аналитические конструкции данного подязыка в сфере речевой деятельности: «говорение», «чтение», «письмо», «аудирование».

В результате изучения дисциплины бакалавр должен обладать следующими общепрофессиональными компетенциями:

ОК-3: способностью уважительно и бережно относиться к историческому наследию и культурным традициям, толерантно воспринимать социальные и культурные различия;

ОК-5: способностью к кооперации с коллегами, работе в коллективе;

ОК-8: способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления;

ОК-9: способностью логически верно, аргументировано и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии;

ОК-10: способностью к чтению и переводу текстов по профессиональной тематике на одном из иностранных языков, владеть им на уровне не ниже разговорного;

ОК-11: способностью к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства.

В результате изучения дисциплины бакалавр должен обладать следующими профессиональными компетенциями:

ПК-1: способностью использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности;

ПК-2: способностью 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;

ПК-3: способностью использовать нормативные правовые документы в своей профессиональной деятельности;

ПК-15: способностью применять программные средства системного, прикладного и специального назначения;

ПК-21: способностью проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов;

ПК-24: способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности.

***Аннотация к рабочей программе дисциплины
«Аппаратные средства вычислительной техники»***

по направлению 090900.62 «Информационная безопасность» (профиль «Безопасность автоматизированных систем»)

Общая трудоемкость дисциплины составляет 5 зачетных единиц.

Форма контроля: экзамен 2 семестр, зачет 3 семестр.

Предполагаемые семестры: 2,3

Целью изучения дисциплины «Аппаратные средства вычислительной техники» является подготовка выпускника к деятельности, связанной с эксплуатацией и обслуживанием оборудования построенного с использованием современных средств вычислительной техники.

Задачами курса является:

- изучение принципов работы элементов цифровых электронных схем;
 - изучение принципов работы узлов ЭВМ;
 - изучение основ проектирования ПЭВМ;
 - изучение архитектуры ПЭВМ различных поколений;
 - изучение системных и периферийных интерфейсов;
 - изучение способов адресации оперативной памяти;
 - изучение структуры и принципов функционирования основных модулей микропроцессорной системы;
- овладение навыками моделирования электронных схем.

Учебная дисциплина относится к циклу БЗ. Для успешного усвоения данной дисциплины необходимо, чтобы студент владел знаниями, умениями и навыками, сформированными в процессе изучения дисциплины «Информатика»: знал системы счисления и представление данных в ЭВМ, состав и назначение функциональных компонентов компьютера; умел использовать программные и аппаратные средства персонального компьютера.

Дисциплина «Аппаратные средства вычислительной техники» обеспечивает изучение дисциплин «Языки программирования», «Операционные системы». Кроме того, знания и практические навыки, полученные в курсе «Аппаратные средства вычислительной техники», используются студентами при изучении естественно-научных дисциплин, а также при разработке курсовых и дипломных работ.

Краткое содержание дисциплины:

История развития средств вычислительной техники.

Методы классификации ЭВМ. Состав вычислительной системы.

Арифметические и логические основы цифровых машин.

Элементы и узлы ЭВМ. Шины ЭВМ. Микропроцессоры. Память.

Периферийные устройства ЭВМ. Рабочие станции, серверы, специализированные ЭВМ. ПЭВМ, АРМ, архитектура серверов. Организация вычислительной сети.

Универсальные и специальные ЭВМ высокой производительности.

Архитектура специализированных вычислительных комплексов и распределенных систем управления.

В результате изучения дисциплины, специалист должен обладать следующими профессиональными компетенциями (ПК):

ОК-8: способность к общению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления;

ПК-2: способностью 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;

ПК-9: способностью принимать участие в эксплуатации подсистем управления информационной безопасности предприятия;

ПК-11: способностью выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации.

Аннотация к рабочей программе дисциплины «Безопасность жизнедеятельности»

**по направлению 090900.62 Информационная безопасность
(профиль «Безопасность автоматизированных систем»)**

Общая трудоемкость дисциплины составляет 3 зачетные единицы.

Форма контроля: зачет.

Предполагаемые семестры: 4.

Целями освоения учебной дисциплины являются: формирование профессиональной культуры безопасности (ноксологической культуры), под которой понимается готовность и способность личности использовать в профессиональной деятельности приобретенную совокупность знаний, умений и навыков для обеспечения безопасности в сфере профессиональной деятельности, характера мышления и ценностных ориентаций, при которых вопросы безопасности рассматриваются в качестве приоритета.

Задачами дисциплины являются: теоретический анализ и разработка методов идентификации опасных и вредных факторов, генерируемых элементами среды обитания (технические средства, технологические процессы, материалы, здания и сооружения, элементы техносферы, природные и социальные явления); разработка принципов и методов защиты от опасностей; разработка и рациональное использование средств защиты человека и среды обитания от негативного воздействия техногенных источников и стихийных явлений; непрерывный контроль и мониторинг среды обитания; моделирование и прогнозирование развития чрезвычайных ситуаций; обучение населения основам защиты от опасностей; разработка мер по ликвидации последствий проявления

опасностей; разработка мер по обеспечению национальной и международной безопасности.

Дисциплина «Безопасность жизнедеятельности» относится к профессиональному циклу дисциплин. Базовые дисциплины: «Математика», «Физика».

Краткое содержание дисциплины:

Человек и среда обитания. Характерные состояния системы "человек – среда обитания".

Основы физиологии труда и комфортные условия жизнедеятельности в техносфере.

Безопасность и экологичность технических систем
Безопасность и экологичность технических систем.

Основы электробезопасности
Основы электробезопасности.

Безопасность систем связи.

Безопасность в чрезвычайных ситуациях.

Управление безопасностью жизнедеятельности.

Анатомо-физиологические и психологические воздействия на человека опасных и вредных факторов при работе с защищенными автоматизированными системами.

В результате изучения дисциплины бакалавр должен обладать следующими профессиональными компетенциями: способностью осуществлять свою деятельность в различных сферах общественной жизни с учетом принятых в обществе моральных и правовых норм (ОК-2); способностью находить организационно-управленческие решения в нестандартных ситуациях и готовности нести за них ответственность (ОК-6);

способностью использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности (ПК-1);

способностью использовать основные методы защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий (ПК-7);

способностью организовать мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств защиты информации (ПК-32).

Аннотация к рабочей программе

дисциплины «Безопасность систем баз данных»

по направлению 090900.62 Информационная безопасность

(профиль «Безопасность автоматизированных систем»).

Общая трудоемкость дисциплины составляет 6 зачетных единиц.

Форма контроля: экзамен.

Предполагаемые семестры: 6,7.

Целями овладение необходимым минимумом знаний по созданию современных систем обработки информации методов защиты информации в системах управления

базами данных. В курсе основное внимание уделяется изложению основных вопросов проектирования проблемно-ориентированных баз данных, ознакомление с системами управления базами данных, возможностям их применения в системах обработки информации, проектированию структур баз данных на концептуальном, логическом, а также физическом уровнях, реализации механизмов защиты данных

Задачами курса являются: формирования целостного представления об основных этапах жизненного цикла баз данных, получение практических навыков разработки приложений с привлечением визуальных средств СУБД и их защиты.

Учебная дисциплина «Безопасность систем баз данных» входит в профессиональный цикл и относится к числу наиболее значимых дисциплин, поскольку служит основой для изучения ключевых учебных дисциплин профессионального цикла.

Знания, полученные по дисциплине «Системы управления базами данных», непосредственно используются при изучении дисциплин:

- Сети и системы передачи информации;
- Технология построения защищенных автоматизированных систем;
- Принципы построения, проектирования и эксплуатации автоматизированных информационных систем;
- Комплексное обеспечение информационной безопасности автоматизированных систем.

Краткое содержание дисциплины:

Понятие СУБД, основные характеристики, функции СУБД

Модели данных

Методология проектирования базы данных

Проектирование реляционной базы данных

Язык манипулирования данными для реляционной модели

Безопасность баз данных

Повышение производительности баз данных

В результате изучения дисциплины бакалавр должен обладать следующими профессиональными компетенциями:

способностью к кооперации с коллегами, работе в коллективе (ОК-5);

способностью находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность (ОК-6);

способностью 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 (ОК-7);

способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления (ОК-8);

способностью логически верно, аргументированно и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии (ОК-9);

способностью к саморазвитию, самореализации, приобретению новых знаний,

повышению своей квалификации и мастерства (ОК-11);

***Аннотация к рабочей программе
дисциплины «Гуманитарные основы информационной безопасности»
по направлению 090900.62 Информационная безопасность
(профиль «Безопасность автоматизированных систем»).***

Общая трудоемкость дисциплины составляет 3 зачетных единиц.

Форма контроля: зачет.

Предполагаемые семестры: 1.

Целями формирование общеметодологических основ обеспечения информационной безопасности, в том числе определение закономерностей развития информационной сферы как существенного фактора жизни современного общества..

Задачами курса являются:

Дать студентам необходимые знания, умения и навыки, в том числе:

- исследование проблем обеспечения баланса интересов личности, общества и государства в информационной сфере;
- прогнозирование социально-психологических последствий внедрения и широкого использования современных информационных технологий;
- создание и развитие системы обеспечения информационно-психологической безопасности от противоправных информационных воздействий на сферы индивидуального, группового и массового сознания.

Учебная дисциплина «Гуманитарные основы информационной безопасности» входит в блок «Гуманитарный, социальный и экономический цикл» и относится к числу дисциплин, обеспечивающих социализацию личности, кроме того она служит основой для изучения учебных дисциплин профессионального цикла.

В дисциплине «Гуманитарные основы информационной безопасности» определяются теоретические основы и практические навыки, при освоении которых студент способен приступить к изучению следующих дисциплин в соответствии с учебным планом:

- теория принятия решений;
- программно-аппаратные средства защиты информации;
- управление информационной безопасностью;
- технология построения защищенных автоматизированных систем;
- информационная безопасность открытых систем;
- технология защиты информации.

Краткое содержание дисциплины:

- Понятие национальной безопасности
- Основные понятия, общеметодологические принципы теории ИБ.
- Анализ угроз ИБ, проблемы информационной войны.
- Государственная информационная политика; проблемы региональной информационной безопасности.

- Методы и средства обеспечения ИБ.

В результате изучения дисциплины бакалавр должен обладать следующими профессиональными компетенциями:

ОК-11: способностью к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства.

ПК-2: способностью 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;

ПК-24: способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности.

Аннотация к рабочей программе дисциплины «Деловой английский язык»

по направлению 090900.62 Информационная безопасность

(профиль «Безопасность автоматизированных систем»).

Общая трудоемкость дисциплины составляет 8 зачетных единиц.

Форма контроля: экзамен

Предполагаемые семестры: 1, 2, 3, 4

Цель: формирование иноязычной компетенции в сфере профессиональной коммуникации. реализуемой в деловом общении с международными партнерами.

Задачами данной дисциплины - обучение студентов активному владению иностранным языком как вторичным средством формирования и формулирования мысли, т.е. умению адекватно намерению и ситуации общения выражать свои мысли на иностранном языке и понимать мысли, выраженные или выражаемые на данном языке. Главной особенностью этого учебного предмета является его профессионально-ориентированный характер: приобретение навыков деловой коммуникации.

Учебная дисциплина «Деловой иностранный язык» относится к вариативной части цикла ГСЭ и оптимально, т.е. в соответствии с компетенциями, обозначенными в ФГОС ВПО, удовлетворяет требованиям гуманитарной и общепрофессиональной системы подготовки бакалавра и рекомендуется в качестве обязательной составляющей подготовки выпускников нефилологических вузов различных направлений. Дисциплина «Деловой иностранный язык» продолжает коммуникативно-ориентированный, профессионально-направленный курс иностранного языка в вузовской системе подготовки.

Дисциплина «Деловой иностранный язык» носит прикладной характер, т.к. её содержание и формы организации учебной деятельности направлены на формирование

иноязычных умений и навыков, реализуемых в виде профессионально-коммуникативных компетенций, соответствующих профессиональным умениям и навыкам, определенным квалификационными характеристиками в рамках данного направления подготовки.

Знания полученные по дисциплине «Деловой иностранный язык», послужат основой формирования навыков информационно-аналитической деятельности, что поможет в изучении дисциплин блока профессиональной подготовки бакалавра.

По окончании курса студент должен:

- знать структуру деловой беседы, правильно использовать речевой этикет, принятый в различных ситуациях международного делового общения;
- уметь реализовывать в процессе делового диалога соответствующие коммуникативные намерения;
- знать структуру презентации, правильно использовать формулы речевого этикета, принятые для вступительной, средней и завершающей частей презентации;
- уметь общаться с графиками, схемами. другими средствами наглядности, используемыми в процессе делового общения;
- уметь составлять план будущего речевого контакта. реализуя в ходе деловой беседы\несложных переговоров определенные коммуникативные намерения;
- формировать цель(и) переговоров, разрабатывать стратегию и тактику переговорного процесса, составлять его план;
- аргументировать свои предложения, убеждая оппонента в целесообразности своего подхода;
- отвечать на возражения партнера по деловому контакту, приводить доводы в пользу того или иного тезиса;
- корректно задавать оппоненту вопросы, направленные на выяснение его позиции, четко отвечать на его возможные вопросы;
- реализовывать в ходе деловых переговоров и презентаций широкий спектр коммуникативных намерений.

Краткое содержание дисциплины:

Темы:

1. Коммуникация. Деловые взаимодействия.
 - а) коммуникативные барьеры: логический барьер, стилистический барьер, семантический барьер.
 - б) слушание и слышание в деловой коммуникации. Вопросы – ответы в деловой коммуникации.
2. Средства деловой коммуникации. Вербальные средства деловой коммуникации:
 - а) приемы деловой коммуникации: речевые клише, речевые штампы;
 - б) официально-деловой стиль речи;
 - в) деловое письмо: речевые конструкции. Речевые шаблоны для делового взаимодействия.
3. Форма деловой коммуникации.
 - а) деловой разговор: деловая беседа, передача информации, аргументирование.

- б) телефонный разговор
- в) деловое совещание
- г) пресс-конференция (несложная)
- д) деловые переговоры

4. Лексико-грамматические особенности делового языка подязыка данного направления:

- лексика: терминология, фразеологизмы, словообразовательные нормы деловой речи, сокращения и аббревиатура

- грамматика:

- а) морфология – трудности в употреблении форм различных частей речи, адекватных коммуникативным намерениям; выбор предлогов; выбор соответствующих грамматических форм времени (таксис и аспект)

- б) синтаксис деловой речи

- порядок слов;

- синтаксис простого и сложного предложений в текстах документов.

5. Типичные ошибки в деловом письме. Редактирование и устранение типичных ошибок в языке и оформлении деловых бумаг.

Данная дисциплина рекомендуется в 2-3 (эффективнее) зачетных единицах.

Основная учебно-информационная база по данной дисциплине представляет собой:

1. раздаточный материал (в соответствии с направлением)- оригинальный материал.
2. учебные пособия, учебники (в большинстве случаев аутентичные) по деловому иностранному языку, деловой коммуникации с CD-дисками.
3. иноязычные отраслевые словари

В результате изучения дисциплины бакалавр должен обладать следующими общепрофессиональными компетенциями:

ОК-3: способностью уважительно и бережно относиться к историческому наследию и культурным традициям, толерантно воспринимать социальные и культурные различия;

ОК-5: способностью к кооперации с коллегами, работе в коллективе;

ОК-8: способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления;

ОК-9: способностью логически верно, аргументировано и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии;

ОК-10: способностью к чтению и переводу текстов по профессиональной тематике на одном из иностранных языков, владеть им на уровне не ниже разговорного;

ОК-11: способностью к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства.

В результате изучения дисциплины бакалавр должен обладать следующими профессиональными компетенциями:

ПК-1: способностью использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем,

возникающих в ходе профессиональной деятельности;

ПК-2: способностью 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;

ПК-3: способностью использовать нормативные правовые документы в своей профессиональной деятельности;

ПК-21: способностью проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов;

ПК-24: способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности.

Аннотация

рабочей программы учебной дисциплины "Дискретная математика"

по направлению 090900.62 Информационная безопасность

(профиль "Безопасность автоматизированных систем").

Общая трудоемкость дисциплины составляет 4 зачетные единицы.

Форма контроля: экзамен.

Предполагаемый семестр: 4

Целью освоения учебной дисциплины является обучение студентов необходимым знаниям и навыкам использования базовых математических моделей и алгоритмов, которые в дальнейшем помогут им профессионально формулировать и решать задачи в конкретных областях информатики и вычислительной техники.

Задачами курса являются: изложение основных положений дискретного анализа, их основных применений в современной математике и информатике; обеспечение возможности изучения в дальнейшем курсов, опирающихся на методы дискретной математики.

Учебная дисциплина "Дискретная математика" входит в математический и естественнонаучный цикл (базовая часть) и относится к числу фундаментальных дисциплин, поскольку служит основой для изучения учебных дисциплин как математического и естественнонаучного, так и профессионального цикла.

Знания, полученные по дисциплине "Дискретная математика", непосредственно используются при изучении дисциплин базового цикла:

- "Математическая логика и теория алгоритмов";
- "Теория вероятностей и математическая статистика";
- "Теория принятия решений";

и дисциплины профессионального цикла:

- "Криптографические методы защиты информации".

Краткое содержание дисциплины:

Метод математической индукции.

Элементы комбинаторики.

Основы теории множеств.

Элементы теории графов.

В результате изучения дисциплины бакалавр должен обладать следующими общекультурными и профессиональными компетенциями:

ОК-9: способность логически верно, аргументировано и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии;

ОК-12: способность критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков;

ПК-1: способность использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности;

ПК-2: 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;

ПК-13: способность к проведению предварительного технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности;

ПК-17: способность к программной реализации алгоритмов решения типовых задач обеспечения информационной безопасности;

ПК-18: способность собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности;

ПК-19: способность составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности;

ПК-20: способность применять методы анализа изучаемых явлений, процессов и проектных решений;

ПК-22: способность проводить эксперименты по заданной методике, обработку результатов, оценку погрешности и достоверности их результатов;

ПК-24: способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности

Аннотация к рабочей программе дисциплины «Дифференциальные уравнения»

по направлению 090900.62 Информационная безопасность

(профиль «Безопасность автоматизированных систем»).

Общая трудоемкость дисциплины составляет 3 зачетные единицы.

Форма контроля: зачет.

Предполагаемые семестры: 2.

Целями освоения учебной дисциплины являются: воспитание математической культуры, развитие навыков математического мышления, обучение применению математических методов и основ математического моделирования в практической деятельности.

Задачами курса являются: формирование целостного представления об основных этапах становления современной математики и математических понятиях и методах, обучение приемам и принципам построения математических моделей и их использованию в профессиональной деятельности.

Учебная дисциплина «Дифференциальные уравнения» входит в математический и естественнонаучный цикл (базовая часть) и относится к числу фундаментальных математических дисциплин, поскольку служит основой для изучения учебных дисциплин как математического и естественнонаучного, так и профессионального цикла.

Знания, полученные по дисциплине «Дифференциальные уравнения», непосредственно используются при изучении дисциплин базового цикла:

- «Вычислительная математика»;

- «Физика»;

и дисциплин профессионального цикла:

- «Электротехника».

Краткое содержание дисциплины:

Дифференциальные уравнения 1-го порядка.

Дифференциальные уравнения 2-го порядка.

Дифференциальные уравнения n-го порядка.

Линейные дифференциальные уравнения n-го порядка.

Системы дифференциальных уравнений.

Приближенные методы решения дифференциальных уравнений.

Краевые задачи для обыкновенных дифференциальных уравнений.

В результате изучения дисциплины бакалавр должен обладать следующими общекультурными и профессиональными компетенциями:

ОК-9: способность логически верно, аргументировано и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии;

ОК-12: способность критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков;

ПК-1: способность использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности;

ПК-2: 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;

ПК-13: способность к проведению предварительного технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности;

ПК-17: способность к программной реализации алгоритмов решения типовых задач обеспечения информационной безопасности;

ПК-18: способность собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности;

ПК-19: способность составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности;

ПК-20: способность применять методы анализа изучаемых явлений, процессов и проектных решений;

ПК-22: способность проводить эксперименты по заданной методике, обработку результатов, оценку погрешности и достоверности их результатов;

ПК-24: способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности.

Аннотация к рабочей программе учебной дисциплины «Документоведение»

по направлению 090900.62 Информационная безопасность (профиль «Безопасность автоматизированных систем»)

Общая трудоёмкость дисциплины составляет 108 зачетных единиц

Форма контроля: экзамен

Предполагаемые семестры: 1 семестр

Цель дисциплины - обеспечить подготовку студентов в области применения вычислительной техники при решении задач документоведения, делопроизводства, управления и анализа хозяйственной деятельности.

Задачи дисциплины - подготовить студентов к самостоятельному использованию ЭВМ при организации делопроизводства и управления в офисе. Изучавшие дисциплину должны: владеть понятиями, связанными с офисной автоматизацией, методами и средствами управления электронными документами, их созданием, хранением, анализом, поиском, организацией коллективного доступа.

Дисциплина относится к циклу БЗ.Б.12. Для освоения дисциплины необходимы знания, полученные при изучении следующих дисциплин:

- Иностранный язык;
- Правоведение;
- Основы управленческой деятельности;
- Русский язык и культура речи;
- Гуманитарные основы информационной безопасности;
- Английский язык в сфере проф.коммуникаций;

- Деловой английский язык;
- Основы информационной безопасности;
- Системы управления базами данных.

Краткое содержание дисциплины:

Документирование. Системы документации и государственные стандарты. Система документов на предприятии. Правила составления и оформления документов. Составление и оформление организационно-распорядительных документов. Деловая переписка. Правила и формы коммерческой переписки с зарубежным партнёром. Документы различного происхождения. Общие принципы организации документооборота на предприятии. Современные офисные технологии обеспечения управленческой деятельности.

В результате изучения дисциплины бакалавр должен обладать следующими компетенциями:

ОК-1: обладать способностью осознавать необходимость соблюдения Конституции Российской Федерации, прав и обязанностей гражданина своей страны, гражданского долга и проявления патриотизма;

ОК-2: обладать способностью осуществлять свою деятельность в различных сферах общественной жизни с учетом принятых в обществе моральных и правовых норм;

ОК-5: обладать способностью к кооперации с коллегами, работе в коллективе;

ОК-6: обладать способностью находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность;

ОК-7: обладать способностью 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;

ОК-8: обладать способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления;

ОК-9: обладать способностью логически верно, аргументировано и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии.

**Аннотация к рабочей программе
дисциплины «Защита информационных ресурсов от внутренних
угроз»**

по направлению подготовки 090900.62 «Информационная безопасность»

(профиль «Безопасность автоматизированных систем»)

Общая трудоемкость дисциплины составляет 5 зачетных единиц

Форма контроля: экзамен

Предполагаемые семестры: 7

Целью изучения дисциплины (модуля) является овладение студентами методами и средствами защиты информационных ресурсов от внутренних угроз.

Задачами курса являются:

- ознакомление с особенностями обеспечения информационной безопасности в корпоративных сетях;
- изучение различных способов аутентификации;
- изучение вопросов обеспечения безопасности информационных ресурсов в различных операционных системах;
- изучение протоколов защищенных каналов;

- ознакомление с технологиями межсетевого экранирования;
- изучение технологии защиты от вредоносных программ;
- ознакомление с методами управления сетевой защитой и системами комплексного управления безопасностью.

Учебная дисциплина относится к циклу БЗ. Для освоения дисциплины необходимы знания, полученные при изучении следующих дисциплин:

- сети и системы передачи информации;
- безопасность операционных систем;
- безопасность вычислительных сетей;
- иностранный язык (английский).

Знания и практические навыки, полученные в результате освоения дисциплины, используются студентами при разработке курсовых и дипломных работ, в научно-исследовательской работе.

Краткое содержание дисциплины

Проблемы информационной безопасности.

Анализ угроз информационной безопасности. Особенности обеспечения информационной безопасности в корпоративных сетях. Тенденции развития ИТ-угроз. Характерные особенности сетевых атак. Угрозы и уязвимости беспроводных сетей.

Политика информационной безопасности. Структура политики безопасности организации. Разработка политики безопасности организации. Стандарты информационной безопасности. Международные и отечественные стандарты информационной безопасности.

Аутентификация.

Идентификация, аутентификация и управление доступом. Аутентификация, авторизация и администрирование действий пользователя. Методы аутентификации, использующие пароли.

Строгая аутентификация. Биометрическая аутентификация пользователя. Управление доступом по схеме однократного входа в авторизацией Single Sign-On. Управление идентификацией и доступом.

Многоуровневая защита информационных ресурсов

Обеспечение безопасности операционных систем. Проблемы обеспечения безопасности ОС. Архитектура подсистемы защиты ОС. Обеспечение безопасности ОС Linux. Обеспечение безопасности ОС Windows 7.

Протоколы защищенных каналов. Защита на канальном уровне – протоколы PPP, L2TP. Защита на сетевом уровне – протокол IPSec. Защита на сеансовом уровне – протоколы SSL, TLS, SOCKS. Защита беспроводных сетей. Технологии межсетевого экранирования. Функции межсетевых экранов. Особенности функционирования межсетевых экранов на различных уровнях модели OSI. Схемы сетевой защиты на базе межсетевых экранов.

Технологии защиты от вредоносных программ. Классификация вредоносных программ. Основы работы антивирусных программ.

Методы управления средствами сетевой защиты. Задачи управления системой сетевой защиты. Архитектура управления средствами сетевой защиты. Аудит и мониторинг безопасности. Обзор современных систем управления сетевой защитой.

Система комплексного управления безопасностью КУБ

Назначение и задачи решаемые системой КУБ. Принципы построения и использования системы КУБ. Формирование и обработка заявок. Конфигурирование системы КУБ. Внедрение и развертывание системы КУБ. Установка программных компонентов системы КУБ. Настройка организационно-штатной структуры. Развертывание агентов на прикладных серверах. Эксплуатация системы КУБ. Обслуживание и дополнительные настройки программных компонентов системы КУБ. Задачи решаемые на этапе

эксплуатации. Аудит событий и отчеты системы КУБ.

В результате изучения дисциплины бакалавр должен обладать следующими профессиональными компетенциями (ПК):

организационно-управленческая деятельность:

ПК-25: способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью;

ПК-26: способностью формировать комплекс мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью.

ПК-27: способностью принимать участие в организации контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации.

ПК-28: способностью изучать и обобщать опыт работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации.

ПК-29: способностью участвовать в работах по реализации политики информационной безопасности.

ПК-30: способностью применять комплексный подход к обеспечению информационной безопасности в различных сферах деятельности.

ПК-31: способностью организовать работу малого коллектива исполнителей с учетом требований защиты информации.

ПК-32: способностью организовать мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств защиты информации.

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.

**Аннотация к рабочей программе дисциплины
«Защита электронного документооборота»
по направлению 090900.62 «Информационная безопасность»
(Профиль «Безопасность автоматизированных систем»)**

Общая трудоемкость дисциплины составляет 3 зачетные единицы.

Форма контроля: зачет.

Предполагаемый семестр: 7.

Целью преподавания дисциплины «Защита электронного документооборота» является: формирование представления об электронном документе как новой сущности в правовых отношениях, предоставление студентам систематизированного подхода к проблеме использования систем электронного документооборота (ЭДО) и информационных систем (ИС) на основе предоставленных базовых сведений.

Задачами курса являются:

- ознакомление с понятиями и методами защищенного ЭДО;
- формирование знаний по современным методам использования систем документооборота с обеспечением юридической значимости обрабатываемой информации;
- формирование навыков применения полученных сведений для решения практических задач при эксплуатации системы Lotus Notes.

Курс «Защита электронного документооборота» относится к разделу Профессionalного цикла учебного плана специальности и содействует формированию у студентов

профессиональных компетенций, необходимых для решения задач, относящихся к профессиональной деятельности в области, соответствующей специализации «Информационная безопасность автоматизированных систем на транспорте»

Для успешного усвоения данной дисциплины необходимо, чтобы студент владел знаниями, умениями и навыками, сформированные в процессе:

- изучения дисциплин: «Криптографические методы защиты информации»; «Программно-аппаратные средства обеспечения ИБ»; «Организационное и правовое обеспечение ИБ».

Краткое содержание дисциплины:

Предмет, цели, содержание дисциплины.

Документы. Документооборот. Информационные системы

Юридическая сила электронных данных. Защита ЭДО

Системы документооборота и их защита

В результате изучения дисциплины, бакалавр должен обладать следующими компетенциями:

ОК-5: способностью к кооперации с коллегами, работе в коллективе;

ПК-3: способностью использовать нормативные правовые документы в своей профессиональной деятельности;

ПК-6: способностью организовывать проведение и сопровождать аттестацию объекта на соответствие государственных или корпоративных нормативных документов;

ПК-14: способностью оформить рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности;

ПК-23: способностью принимать участие в проведении экспериментально-исследовательских работ систем защиты информации с учетом требований по обеспечению информационной безопасности;

ПК-30: способностью применять комплексный подход к обеспечению информационной безопасности в различных сферах деятельности;

ПК-32: способностью организовать мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств защиты информации;

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.

**Аннотация к рабочей программе
дисциплины «Иностранный язык»**

по направлению 090900.62 Информационная безопасность

(профиль «Безопасность автоматизированных систем»).

Общая трудоемкость дисциплины составляет 7 зачетных единиц.

Форма контроля: экзамен.

Предполагаемые семестры: 1, 2, 3.

Целью освоения учебной дисциплины «Иностранный язык» в рамках данной рабочей программы является формирование практического владения иностранным

языком как вторичным средством общения в виде полного понимания содержания текстов при чтении и извлечении из них необходимой информации, а также участия в варьирующихся ситуациях устного и письменного общения с определенным коммуникативным намерением, относящихся к социально-общественной, учебно-производственной, страноведческой, бытовой и профессионально-ориентированной сферам деятельности. В процессе достижения этой цели реализуются образовательная и воспитательная цели, входящие составной частью в вузовскую программу гуманитаризации высшего образования и направленные на становление всесторонне развитой личности, обладающей способностью логически и креативно мыслить, умением собирать, анализировать и ранжировать информацию в зависимости от поставленной задачи, достаточной эрудицией в области историко-культурного наследия страны изучаемого языка, культурой речи.

Задачи дисциплины «Иностранный язык»: унифицировать полученные в школе умения и навыки чтения на расширенном языковом материале; совершенствовать эти навыки с целью подготовки к различным видам чтения; сформировать навыки понимания речи собеседника в ситуациях общения: реплики, клише, фразы, монологические высказывания (объем высказывания 200-240 слов при темпе речи до 200 слогов в минуту); развить навык диалогической речи: обмен репликами (объем не менее 4-5 высказываний); сформировать навык подготовки собственного сообщения (объем не менее 8-10 фраз. Темп речи – до 200 слогов в минуту).

Учебная дисциплина «Иностранный язык» относится к базовой части цикла ГСЭ и является гуманитарной и общепрофессиональной основой системы подготовки выпускника технического вуза. Знания полученные по дисциплине «Иностранный язык», являются инструментом для получения информации о международных стандартах и достижениях в области будущей профессиональной деятельности. В данной программе предусматривается преемственность вузовского и школьного обучения иностранному языку. Дисциплина «Иностранный язык» рассматривается как составной элемент системы иноязычной подготовки выпускника учебного заведения, представляющей собой следующую последовательность этапов изучения иностранного языка: бакалавриат/специалитет – магистратура – аспирантура. Последовательность изучения дисциплин в зависимости от этапов обучения иностранному языку представляет собой следующее: «Иностранный язык» - «Деловой иностранный язык» - «Иностранный язык в сфере профессиональной коммуникации», что позволяет реализовать принцип преемственности данных дисциплин, направленный на последовательное раскрытие и объективацию особенностей осваиваемого (иноязычного) языкового сознания. Профессиональная коммуникация на иностранном языке является конечным результатом его изучения в вузе.

Знания, полученные в ходе изучения данной дисциплины, могут использоваться при изучении дисциплин социально-гуманитарного цикла (история отечества, логика, философия), а также дисциплин общепрофессионального и профессионального циклов.

Краткое содержание дисциплины:

а) фонетика

- понятие артикуляционной базы языка и осязаемые моменты артикуляции;
- ритмика (ударность и безударность);
- паузация и виды синтаксической связи;
- интонация незавершенности и завершенности (с опорой на внешнюю наглядность);
- логическое ударение (с опорой на внешнюю наглядность);

б) грамматика

- минимизация и строгая последовательность в подаче грамматического материала в моделированных текстах – образцах;
- порядок слов (общее предоставление, минимизация);
- множественное число существительных;
- артикль (наиболее употребительные случаи без исключений);
- формальное подлежащее;
- степени сравнения прилагательных и наречий;
- глагол: группа времен Indefinite, Continuous, Perfect.

Основные отличительные особенности. Действительный залог, страдательный залог (оба с минимизацией и отбором наиболее употребительных случаев);

- причастие действительное и страдательное. Причастный оборот;
- модальные глаголы (минимизация);
- неличные формы глагола (минимизация);
- все виды вопросительных предложений (кроме риторических);

в) лексика и фразеология

- минимизация в отборе лексики, представляющей стиль научного общения;
- тенденция к беспереводной подаче лексики с опорой на наглядность;
- накопление словаря за счет терминологии и словосочетаний.

В результате изучения дисциплины бакалавр должен обладать следующими общепрофессиональными компетенциями:

ОК-3: способностью уважительно и бережно относиться к историческому наследию и культурным традициям, толерантно воспринимать социальные и культурные различия;

ОК-5: способностью к кооперации с коллегами, работе в коллективе;

ОК-8: способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления;

ОК-9: способностью логически верно, аргументированно и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии;

ОК-10: способностью к чтению и переводу текстов по профессиональной тематике на одном из иностранных языков, владеть им на уровне не ниже разговорного;

ОК-11: способностью к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства.

В результате изучения дисциплины бакалавр должен обладать следующими профессиональными компетенциями:

ПК-2: способностью 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;

ПК-3: способностью использовать нормативные правовые документы в своей профессиональной деятельности;

ПК-21: способностью проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов;

ПК-24: способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности.

**Аннотация к рабочей программе дисциплины
«Информационная безопасность открытых систем»
по направлению 090900.62 «Информационная безопасность»
(Профиль «Безопасность автоматизированных систем»)**

Общая трудоемкость дисциплины составляет 3 зачетные единицы.

Форма контроля: зачет.

Предполагаемый семестр: 7.

Цель освоения дисциплины «ИБ открытых систем» состоит:

- в изучении способов разработки и реализации мер по защите информационных ресурсов автоматизированных открытых систем (АОС);
- в решении задач, требующих классификации и структуризации мер обеспечения безопасности АОС от степени конфиденциальности.

Задачами курса являются:

- освоение принципов организации информационных систем в соответствии с требованиями по защите информации;
- ознакомление с основными нормативно-правовыми актами в области ИБ и защиты, а также нормативными методическими документами ФСБ РФ;
- умение анализировать и оценивать угрозы ИБ объекта;
- умение применять отечественные и зарубежные стандарты в области ИБ для проектирования, разработки и оценки защищенности открытых АС;
- освоение методов и средств выявления угроз безопасности АС;
- овладение навыками организации и обеспечения режима секретности, а также методами технической защиты информации.

Дисциплина является самостоятельным элементом в системе подготовки специалиста, относится к циклу БЗ.ДВ2.1. Для освоения дисциплины необходимы знания, полученные при изучении следующих дисциплин:

- основы информационной безопасности;
- принципы построения, проектирования и эксплуатации АИС;
- теоретические основы компьютерной безопасности.

В дисциплине «Информационная безопасность открытых систем» определяются теоретические основы и практические навыки, при освоении которых студент способен приступить к изучению следующих дисциплин в соответствии с учебным планом:

- комплексное обеспечение информационной безопасности АС;
- интегрированные информационные системы в управлении.

Краткое содержание дисциплины:

- Технологии автоматизированных открытых систем (АОС).
- Стандартизация подходов к обеспечению информационной безопасности АОС.
- Составляющие информационной безопасности АОС.

- Интеграция средств информационной безопасности в технологическую среду.
- Технологии и инструменты обеспечения безопасности информации в АОС

В результате изучения дисциплины, бакалавр должен обладать следующими компетенциями:

ОК-5: способностью к кооперации с коллегами, работе в коллективе;

ОК-6: способностью находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность;

ОК-7: способностью 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.

ОК-8: способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления;

ОК-9: способностью логически верно, аргументировано и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии.

ПК-1: способностью использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности.

ПК-2: способностью 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.

ПК-3: способностью использовать нормативные правовые документы в своей профессиональной деятельности.

ПК-4: способностью формировать комплекс мер по информационной безопасности с учетом 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 учетом 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;

ПК-7: способностью использовать основные методы защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий.

ПК-8: способностью 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.

ПК-9: способностью принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия.

ПК-10: способностью администрировать подсистемы информационной безопасности объекта.

ПК-11: способностью выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации.

ПК-12: способностью участвовать в разработке подсистемы управления информационной безопасностью.

ПК-13: способностью к проведению предварительного технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности.

ПК-14: способностью оформить рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности.

ПК-15: способностью применять программные средства системного, прикладного и специального назначения.

ПК-16: способностью использовать инструментальные средства и системы программирования для решения профессиональных задач.

ПК-17: способностью к программной реализации алгоритмов решения типовых задач обеспечения информационной безопасности.

ПК-18: способностью собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности.

ПК-19: способностью составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности.

ПК-20: способностью применять методы анализа изучаемых явлений, процессов и проектных решений.

ПК-21: способностью проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов.

ПК-22: способностью проводить эксперименты по заданной методике, обработку результатов, оценку погрешности и достоверности их результатов.

ПК-23: способностью принимать участие в проведении экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности.

ПК-24: способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности.

ПК-25: способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью.

ПК-26: способностью формировать комплекс мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью.

ПК-27: способностью принимать участие в организации контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации.

ПК-28: способностью изучать и обобщать опыт работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации.

ПК-29: способностью участвовать в работах по реализации политики информационной безопасности.

ПК-30: способностью применять комплексный подход к обеспечению информационной безопасности в различных сферах деятельности.

ПК-31: способностью организовать работу малого коллектива исполнителей с учетом требований защиты информации.

ПК-32: способностью организовать мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств защиты информации.

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.

**Аннотация к рабочей программе
дисциплины «Информатика»
для направления подготовки 090900.62 Информационная безопасность
(профиль «Безопасность автоматизированных систем»; уровень ООП «бакалавр»)**

Общая трудоемкость дисциплины составляет 3 зачетных единицы.

Форма контроля: зачет.

Предполагаемые семестры: 1.

Целью курса является формирование общей информационной культуры студентов, подготовка их к деятельности, связанной с использованием современных информационных технологий.

Задачами курса являются изучение основных понятий информатики; изучение свойств и способов записи алгоритмов; изучение способов представления чисел, символов, графики, аудио- и видеoinформации в персональном компьютере; ознакомление с логическими основами устройства ЭВМ; ознакомление с составом и назначением функциональных узлов компьютера; изучение основ построения компьютерных сетей.

Учебная дисциплина «Информатика» в основной образовательной программе подготовки специалистов находится в блоке математических и естественнонаучных дисциплин.

Знания, полученные по дисциплине «Информатика», непосредственно используются при изучении дисциплин:

- «Методы программирования»,
- «Аппаратные средства вычислительной техники»,
- «Основы информационной безопасности»,
- «Программно-аппаратные средства защиты информации»,
- «Сети и системы передачи информации»

Краткое содержание дисциплины:

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

В результате изучения дисциплины выпускник должен обладать следующими общекультурными (ОК) и профессиональными компетенциями (ПК):

- **ОК-8:** способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления;
- **ОК-11:** способностью к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства;
- **ПК-1:** способность использовать основные естественно научные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности;
- **ПК-8:** 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;

- **ПК-11:** способностью выполнять работы по установке, настройке и обслуживанию технических и программно – аппаратных средств защиты информации);
- **ПК-18:** способностью собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности;
- **ПК- 19:** способностью составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности;
- **ПК – 24:** способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности.

Аннотация к рабочей программе

дисциплины «Информатика 2 (Языки программирования)»

по направлению 090900.62 Информационная безопасность

Общая трудоемкость дисциплины составляет 180 часов 5 зачетных единиц

Форма контроля: экзамен

Предполагаемые семестры: 1

Целями освоения учебной дисциплины являются: подготовка студентов к деятельности, связанной с разработкой программного обеспечения для решения профессиональных задач.

Задачами курса являются: 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.

Учебная дисциплина «Информатика 2 (Языки программирования)» входит в цикл Б2. Знания и практические навыки, полученные из курса «Информатика 2 (Языки программирования)», используются обучаемыми при изучении дисциплин:

- «Технологии и методы программирования»;
- «Программно-аппаратные средства защиты информации»;
- «Криптографические методы защиты информации»;
- «Безопасность систем баз данных».

Краткое содержание дисциплины

Язык Object Pascal и среда программирования Borland Delphi

Основы объектно-ориентированного программирования

Графика

В результате изучения дисциплины бакалавр должен обладать следующими профессиональными компетенциями:

ПК-15: способен применять программные средства системного, прикладного и

специального назначения;

ПК-16: способен использовать инструментальные средства и системы программирования для решения профессиональных задач;

ПК-17: способен к программной реализации алгоритмов решения типовых задач обеспечения информационной безопасности.

**Аннотация к рабочей программе
дисциплины «Информационно-аналитическая
работа по обеспечению информационной безопасности АС»
по направлению 090900.62 «Информационная безопасность» (профиль
«Безопасность АС»)**

Общая трудоемкость дисциплины составляет 6 зачетных единиц.

Форма контроля: курсовой проект, зачет, экзамен.

Предполагаемые семестры: 6,7.

Целью курса является сформировать знания о принципах и методах информационно-аналитической работы, отработать навыки по их использованию для обеспечения информационной безопасности АС, а также познакомить с современными технологиями аналитической разведки и принятия решений по результатам ИАР.

Задачами курса являются: рассмотрение основных понятий, принципов, этапов и особенностей сферы информационно-аналитической работы;

получение характеристики современного информационного общества, проблем защиты информации и обеспечения информационной безопасности;

формирование у студентов навыков написания информационных обзоров и аналитических справок, а также разработки проектов; развитие у студентов навыков участия и организации информационно-аналитической работы.

Учебная дисциплина «Информационно-аналитическая работа по обеспечению информационной безопасности АС» в основной образовательной программе подготовки специалистов находится в блоке математических и естественнонаучных дисциплин.

Знания, полученные по дисциплине «Информационно-аналитическая работа по обеспечению информационной безопасности АС», непосредственно используются при изучении дисциплин:

«Безопасность операционных систем»

«Аппаратные средства вычислительной техники»

«Основы информационной безопасности»

«Программно-аппаратные средства защиты информации»

«Системы сети и передачи информации».

Краткое содержание дисциплины:

Информационное общество

Информационно - аналитическая работа

Источники информации для ведения ИАР

Технологии информационно-поисковой работы

Методы оценки достоверности и новизны информации

Технологии информационно-аналитической работы

Безопасность информационно-аналитической работы

Инструментарий для ведения информационно-аналитической работы

В результате изучения дисциплины выпускник должен обладать следующими общекультурными (ОК) и профессиональными компетенциями (ПК):

ОК-5: способностью к кооперации с коллегами, работе в коллективе;

ОК-6: способностью находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность;

ОК-7: способностью 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;

ОК-8: способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления;

ОК-9: способностью логически верно, аргументированно и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии;

ПК-1: способностью применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами;

ПК-15: способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере своей профессиональной деятельности

ПК-16: способностью применять современные методы исследования с использованием компьютерных технологий;

ПК-18: способностью проводить анализ рисков информационной безопасности автоматизированной системы.

**Аннотация к рабочей программе
дисциплины «Информационные технологии»
по направлению 090900.62 Безопасность АС
(профиль «Безопасность АС»).**

Общая трудоемкость дисциплины составляет 3 зачетные единицы.

Форма контроля: зачет.

Предполагаемые семестры: 5

Целями освоения дисциплины «Информационные технологии» являются:

- получение системного представления о современных информационных технологиях;
- приобретение знаний об основных видах систем обработки информации и их характеристиках;
- формирование навыков по построению и использованию перспективных сетевых технологий, стандартов и протоколов передачи данных.

Задачи дисциплины «Информационные технологии»:

изучение основ администрирования вычислительных сетей; принципы построения информационных систем; осуществлять меры противодействия нарушениям сетевой безопасности; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем.

Учебная дисциплина относится к циклу БЗ.ДВ.8. Для освоения дисциплины необходимы знания, полученные при изучении следующих дисциплин:

- математика;
- физика;
- информатика.

В дисциплине «Информационные технологии» определяются теоретические основы и практические навыки, при освоении которых студент способен приступить к изучению следующих дисциплин в соответствии с учебным планом:

- программно-аппаратные средства защиты информации;
- технология построения защищенных автоматизированных систем.

Краткое содержание дисциплины:

Основные понятия математического моделирования.

Модели задач линейного программирования.

Основные понятия теории оптимизации. Задачи оптимизации производственных процессов, планирования производства и распределения ресурсов. Построение математических моделей задач. Симплексный метод решения задач. Модели теории игр. Задачи оптимизации на графах.

В результате изучения дисциплины бакалавр должен обладать следующими общими и профессиональными компетенциями:

ОК-8: способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления.

ПК-2: способностью 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.

ПК-8: способностью 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.

ПК-9: способностью принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия.

ПК-10: способностью администрировать подсистемы информационной безопасности объекта.

ПК-11: способностью выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации.

ПК-12: способностью участвовать в разработке подсистемы управления информационной безопасностью.

ПК-15: способностью применять программные средства системного, прикладного и специального назначения.

ПК-16: способностью использовать инструментальные средства и системы программирования для решения профессиональных задач.

ПК-17: способностью к программной реализации алгоритмов решения типовых задач обеспечения информационной безопасности.

ПК-18: способностью собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности.

ПК-22: способностью проводить эксперименты по заданной методике, обработку результатов, оценку погрешности и достоверности их результатов.

ПК-24: способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности.

ПК-27: способностью принимать участие в организации контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации.

**Аннотация к рабочей программе
дисциплины «Исследование операций»
по направлению 090900.62 Безопасность АС
(профиль «Безопасность АС»).**

Общая трудоемкость дисциплины составляет 3 зачетные единицы.

Форма контроля: зачет.

Предполагаемые семестры: 4

Цель изучения дисциплины заключается в формировании у студентов способности при решении профессиональных задач анализировать предметную область и процессы с применением методов системного анализа и математического моделирования, ставить и решать оптимизационные задачи с использованием современных информационно-коммуникационных технологий.

Задачи дисциплины «Исследование операций»:

- 1) ознакомить студентов с основными понятиями математического моделирования, с классификацией моделей;
- 2) ознакомить с различными типами прикладных задач, существующими алгоритмами решения и разработанными математическими методами исследования оптимизационных проблем
- 3) познакомиться с современными информационными технологиями, пакетами прикладных программ, приложениями и средствами, которые применяются для

моделирования и реализации построенных алгоритмов решения задач, в том числе в профессиональной среде.

- 4) научить определять принадлежность задачи к определенному типу, приводить задачу к известной форме и использовать имеющиеся готовые алгоритмы, как для аналитического, так и для компьютерного решения.

Учебная дисциплина «Исследование операций» относится к циклу дисциплины по выбору (Б2.ДВ2).

Изучение дисциплины «Исследование операций» базируется на дисциплинах: «Математика (алгебра)», «Дискретная математика», «Теория вероятностей и математическая статистика», «Математическая логика и теория алгоритмов».

Знания и практические навыки, полученные из дисциплины «Исследование операций», используются обучаемыми при разработке курсовых и дипломных работ.

Краткое содержание дисциплины:

Основные понятия математического моделирования.

Модели задач линейного программирования.

Основные понятия теории оптимизации. Задачи оптимизации производственных процессов, планирования производства и распределения ресурсов. Построение математических моделей задач. Симплексный метод решения задач. Модели теории игр. Задачи оптимизации на графах.

В результате изучения дисциплины бакалавр должен обладать следующими общими и профессиональными компетенциями:

ОК-5: способностью к кооперации с коллегами, работе в коллективе;

ОК-6: способностью находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность;

ОК-7: способностью осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности, готовностью и способностью к активной созидательной деятельности в условиях информационного противоборства;

ОК-12: способностью критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков;

ПК-1: способностью использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности;

ПК-2: способностью 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;

ПК-15: способностью применять программные средства системного, прикладного и

специального назначения;

ПК-16: способностью использовать инструментальные средства и системы программирования для решения профессиональных задач.

Аннотация

**к рабочей программе учебной дисциплине «История»
по направлению 090900 «Информационная безопасность» (профиль
«Безопасность автоматизированных систем»)**

Общая трудоемкость дисциплины составляет 3 зачетных единиц.

Форма контроля: экзамен.

Предполагаемые семестры: 1.

Целями освоения учебной дисциплины являются

- дать понятие об истории и ее месте в системе знаний и в системе гуманитарных наук;

- познакомить студентов с основными этапами развития Отечественной и Всемирной истории и важнейшими событиями;

- изучить специфику исторического процесса в России и мире;

- помочь сформировать у молодых специалистов на исторических примерах высоких моральных и нравственных качеств, уважения и любви к Отечеству и активной жизненной позиции;

- расширить кругозор, научить грамотно и красиво выстраивать речь, привить любовь к исторической литературе.

Задачи:

дать студентам необходимые знания, умения и навыки, в том числе:

– формирование мировоззрения у молодых специалистов,

- ориентация в исторических событиях;

- понимание причинно-следственные связи тех или иных событий;

- анализ и критический разбор исторических событий.

Учебная дисциплина «История» входит в социогуманитарный цикл и относится к числу фундаментальных исторических дисциплин.

Знания, полученные по дисциплине «История», непосредственно используются при изучении дисциплин базового цикла:

- «Философия»,

- «Политология»,

- «Экономика»,

- «Логика»,

- «Социология».

Краткое содержание дисциплины:

Основы истории Древнего мира, Средних веков, Нового времени.

История Киевской Руси.

История Московского царства.

История Императорской России.

История СССР.

Россия на современном этапе.

В результате изучения дисциплины бакалавр должен обладать следующими общекультурными компетенциями:

ОК-1 – способностью осознавать необходимость соблюдения конституции Российской Федерации, прав и обязанностей гражданина своей страны, гражданского долга и проявление патриотизма.

ОК-3 – способностью уважительно и бережно относиться к историческому наследию и культурным традициям, толерантно воспринимать социальные и культурные различия.

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.

ОК-5 – способностью к кооперации с коллегами, работе в коллективе.

ОК-12 – способностью критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков.

ОК-13 – способностью к самостоятельному применению методов физического воспитания для повышения адаптационных резервов организма и укрепления здоровья, готовностью к достижению должного уровня физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности.

**Аннотация к рабочей программе дисциплины
«Катастрофоустойчивость информационных систем»
по направлению 090900.62 «Информационная безопасность»
(Профиль «Безопасность автоматизированных систем»)**

Общая трудоемкость дисциплины составляет 2 зачетных единицы.

Форма контроля: зачет.

Предполагаемый семестр: 7.

Цели освоения дисциплины « Катастрофоустойчивость информационных систем» состоят:

- в изучении способов разработки и реализации мер по защите информационных ресурсов автоматизированных информационных систем (АИС);
- в решении задач, требующих классификации и структуризации мер обеспечения безопасности АИС, повышения отказоустойчивости и катастрофоустойчивости.

Задачами курса являются:

- освоение принципов построения информационных систем;
- ознакомление с принципами организации информационных систем в соответствии с требованиями по защите информации;
- изучение основных нормативно-правовых актов в области информационной безопасности и защиты, а также нормативных методических документы Федеральной службы безопасности Российской Федерации.

Дисциплина является самостоятельным элементом в системе подготовки специалиста, относится к циклу БЗ.ДВ4.2. Для освоения дисциплины необходимы знания, полученные при изучении следующих дисциплин:

- основы информационной безопасности;
- теоретические основы компьютерной безопасности;
- принципы построения, проектирования и эксплуатации автоматизированных информационных систем.

В дисциплине «Катастрофоустойчивость информационных систем» определяются теоретические основы и практические навыки, при освоении которых студент способен приступить к изучению следующих дисциплин в соответствии с учебным планом:

- комплексное обеспечение информационной безопасности автоматизированных систем;
- интегрированные информационные системы в управлении.

Краткое содержание дисциплины:

Проблемы обеспечения безопасности автоматизированных информационных систем (АИС).

Надежность и катастрофоустойчивость АИС

Методы обеспечения безотказности и высокой готовности АИС.

Особенности использования кластерных технологий в АИС с высоким показателем готовности.

Модели оценки катастрофоустойчивости АИС

В результате изучения дисциплины, бакалавр должен обладать следующими компетенциями:

ОК-5: способностью к кооперации с коллегами, работе в коллективе;

ОК-6: способностью находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность;

ОК-7: способностью 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.

ОК-8: способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления;

ОК-9: способностью логически верно, аргументировано и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии.

ПК-1: способностью использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности.

ПК-2: способностью 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.

ПК-3: способностью использовать нормативные правовые документы в своей профессиональной деятельности.

ПК-4: способностью формировать комплекс мер по информационной безопасности с учетом 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 учетом 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;

ПК-7: способностью использовать основные методы защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий.

ПК- 8: способностью 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.

ПК-19: способностью составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности.

ПК-20: способностью применять методы анализа изучаемых явлений, процессов и проектных решений.

ПК-21: способностью проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов.

ПК-22: способностью проводить эксперименты по заданной методике, обработку результатов, оценку погрешности и достоверности их результатов.

ПК-23: способностью принимать участие в проведении экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности.

ПК-24: способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности.

**Аннотация к рабочей программе
Дисциплины «Комплексное обеспечение информационной
безопасности автоматизированных систем»
по направлению 090900.62 Информационная безопасность
профиль «Безопасность автоматизированных систем»**

Общая трудоемкость дисциплины составляет 4 зачетные единицы

Форма контроля: экзамен

Предполагаемые семестры: 8

Целями освоения дисциплины « Комплексное обеспечение информационной безопасности автоматизированных систем» состоят:

- в изучении способов разработки и реализации мер по защите информационных ресурсов автоматизированных систем (АС);

- в решении задач, требующих классификации и структуризации мер обеспечения безопасности АС от степени конфиденциальности.

Задачами курса являются: анализ и оценка угрозы информационной безопасности объекта; применение отечественных и зарубежных стандартов в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем. Изучение принципов построения и организации информационных систем в соответствии с требованиями по защите информации; основных нормативных правовых актов в области информационной безопасности и защиты, а также нормативных методических документов ФСБ РФ; мер противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты.

Учебная дисциплина «Комплексное обеспечение ИБ АС» является самостоятельным элементом в системе подготовки специалиста, относится к циклу БЗ.ДВЗ.1. Для освоения дисциплины необходимы знания, полученные при изучении

следующих дисциплин:

- основы информационной безопасности;
- принципы построения, проектирования и эксплуатации автоматизированных информационных систем;
- информационная безопасность открытых систем.

В дисциплине «Комплексное обеспечение информационной безопасности автоматизированных систем» определяются теоретические основы и практические навыки, при освоении которых студент способен приступить к изучению следующих дисциплин в соответствии с учебным планом:

- интегрированные информационные системы в управлении.

Краткое содержание дисциплины

Постановка проблемы комплексного обеспечения информационной безопасности АС. Состав компонентов комплексной системы обеспечения информационной безопасности (КСИБ). Интеграция средств информационной безопасности в технологическую среду. Стадии и этапы создания КСИБ. Типовая структура программно-технического комплекса. Методы и методики оценки качества КСИБ. Аттестация и сертификация систем и средств защиты информации.

В результате изучения дисциплины специалист должен обладать следующими профессиональными компетенциями:

ОК-1: способностью осознавать необходимость соблюдения Конституции РФ, прав и обязанностей гражданина своей страны, гражданского долга и проявления патриотизма.

ОК-2: способностью осуществлять свою деятельность в различных сферах общественной жизни с учетом принятых в обществе моральных и правовых норм;

ПК-25: способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью.

ПК-26: способностью формировать комплекс мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью.

ПК-27: способностью принимать участие в организации контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации.

ПК-28: способностью изучать и обобщать опыт работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации.

ПК-29: способностью участвовать в работах по реализации политики информационной безопасности.

ПК-30: способностью применять комплексный подход к обеспечению информационной безопасности в различных сферах деятельности.

ПК-31: способностью организовать работу малого коллектива исполнителей с учетом требований защиты информации.

ПК-32: способностью организовать мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств защиты информации.

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.

**Аннотация к рабочей программе
дисциплины «Математика. Алгебра и геометрия»
по направлению 090900.62 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
(Профиль подготовки - Безопасность автоматизированных систем).**

Общая трудоемкость дисциплины составляет 6 зачетных единиц.

Форма контроля: экзамен.

Предполагаемые семестры: 1,2.

Основной целью дисциплины является вооружение будущих специалистов прочными знаниями, умениями и навыками в области алгебры и геометрии, позволяющими им успешно справляться с задачами профессиональной деятельности.

Основными задачами дисциплины являются:

1) формирование у студентов теоретических знаний и умений, необходимых для изучения других разделов математики, в частности, математического анализа и дифференциальных уравнений;

2) формирование у студентов теоретических знаний и умений, необходимых для изучения дисциплин профессиональной подготовки, в частности, дисциплины «Криптографические методы защиты информации».

В связи с последней задачей кроме традиционного изучения комплексных чисел, систем линейных уравнений, матриц и определителей, векторных и евклидовых пространств, линейных преобразований, присутствующего в программах по дисциплине «Высшая математика» практически во всех технических вузах, в программу включены нетрадиционные для таких вузов темы. В частности, программа предусматривает изучение элементов теории чисел, элементов теории групп, колец, полей, играющих большую роль при линейном и циклическом кодировании и в криптографии.

Учебная дисциплина «Математика. Алгебра и геометрия» входит в математический и естественнонаучный цикл (базовая часть) и относится к числу фундаментальных математических дисциплин, поскольку служит основой для изучения учебных дисциплин как математического и естественнонаучного, так и профессионального цикла.

Знания, полученные по дисциплине «Математика. Алгебра и геометрия», непосредственно используются при изучении дисциплин базового цикла:

- «Математика. Математический анализ»;
 - «Дифференциальные уравнения»;
 - «Математическая логика и теория алгоритмов»;
 - «Дискретная математика»;
 - «Теория вероятностей и математическая статистика»;
 - «Теория автоматов»;
 - «Физика»;
 - «Информатика»;
- и дисциплин профессионального цикла:
- «Электротехника»;
 - «Электроника и схемотехника»,
 - «Криптографические методы защиты информации».

Краткое содержание дисциплины:

Элементы линейной алгебры (часть 1).

- Элементы векторной алгебры.
- Аналитическая геометрия на плоскости.
- Аналитическая геометрия в пространстве.
- Основные алгебраические структуры.
- Элементы линейной алгебры (часть 2).

В результате изучения дисциплины бакалавр должен обладать следующими общекультурными и профессиональными компетенциями:

ОК-9: способность логически верно, аргументированно и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии;

ОК-12: способность критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков;

ПК-1: способность использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности;

ПК-2: 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;

ПК-13: способность к проведению предварительного технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности;

ПК-17: способность к программной реализации алгоритмов решения типовых задач обеспечения информационной безопасности;

ПК-18: способность собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности;

ПК-19: способность составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности;

ПК-20: способность применять методы анализа изучаемых явлений, процессов и проектных решений;

ПК-22: способность проводить эксперименты по заданной методике, обработку результатов, оценку погрешности и достоверности их результатов;

ПК-24: способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности.

**Аннотация к рабочей программе
дисциплины «Математика. Математический анализ»
по направлению 090900.62 Информационная безопасность
(профиль «Безопасность автоматизированных систем»).**

Общая трудоемкость дисциплины составляет 5 зачетных единиц.

Форма контроля: экзамен, зачет.

Предполагаемые семестры: 1,2.

Целями освоения учебной дисциплины являются: воспитание математической культуры, развитие навыков математического мышления, обучение применению математических методов и основ математического моделирования в практической деятельности.

Задачами курса являются: формирование целостного представления об основных этапах становления современной математики и математических понятиях и методах, обучение приемам и принципам построения математических моделей и их использованию в профессиональной деятельности.

Учебная дисциплина «Математика. Математический анализ» входит в математический и естественнонаучный цикл (базовая часть) и относится к числу фундаментальных математических дисциплин, поскольку служит основой для изучения учебных дисциплин как математического и естественнонаучного, так и профессионального цикла.

Знания, полученные по дисциплине «Математика. Математический анализ», непосредственно используются при изучении дисциплин базового цикла:

- «Дифференциальные уравнения»;
 - «Дискретная математика»;
 - «Теория вероятностей и математическая статистика»;
 - «Вычислительная математика»;
 - «Физика»;
 - «Информатика»;
- и дисциплин профессионального цикла:
- «Электротехника»;
 - «Электроника и схемотехника».

Краткое содержание дисциплины:

Введение в математический анализ.

Дифференциальное исчисление функции одной переменного.

Функции многих переменных.

Интегральное исчисление функции одной переменной.

Ряды.

В результате изучения дисциплины бакалавр должен обладать следующими общекультурными и профессиональными компетенциями:

ОК-9: способность логически верно, аргументировано и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии;

ОК-12: способность критически оценивать свои достоинства и недостатки,

определять пути и выбрать средства развития достоинств и устранения недостатков;

ПК-1: способность использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности;

ПК-2: 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;

ПК-13: способность к проведению предварительного технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности;

ПК-17: способность к программной реализации алгоритмов решения типовых задач обеспечения информационной безопасности;

ПК-18: способность собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности;

ПК-19: способность составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности;

ПК-20: способность применять методы анализа изучаемых явлений, процессов и проектных решений;

ПК-22: способность проводить эксперименты по заданной методике, обработку результатов, оценку погрешности и достоверности их результатов;

ПК-24: способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности.

**Аннотация к рабочей программе
дисциплины «Методы программирования (СИ)»
по направлению 090900.62 Информационная
безопасность(профиль«Безопасность автоматизированных систем»)**

Общая трудоемкость дисциплины составляет 144 часа 4 зачетные единицы

Форма контроля: экзамен

Предполагаемые семестры: 2

Целями освоения учебной дисциплины являются: подготовка студентов к деятельности, связанной с разработкой программного обеспечения для решения профессиональных задач.

Задачами курса являются: развитие у студентов логического мышления, способности математической формализации прикладных задач, создания алгоритмов и их

анализа, овладения навыками программной реализации алгоритмов.

Учебная дисциплина «Методы программирования (СИ)» входит в цикл БЗ. Знания и практические навыки, полученные из курса «Методы программирования (СИ)», используются обучаемыми при изучении дисциплин:

- «Программно-аппаратные средства защиты информации»;
- «Криптографические методы защиты информации».

Краткое содержание дисциплины

Структуры данных

Программная реализация алгоритмов

Алгоритмы сортировки

В результате изучения дисциплины бакалавр должен обладать следующими профессиональными компетенциями:

ПК-15: способен применять программные средства системного, прикладного и специального назначения;

ПК-16: способен использовать инструментальные средства и системы программирования для решения профессиональных задач;

ПК-17: способен к программной реализации алгоритмов решения типовых задач обеспечения информационной безопасности.

Аннотация к рабочей программе дисциплины «Методы выявления нарушений информационной безопасности, аттестация автоматизированных систем» по направлению 090900.62 «Информационная безопасность» (профиль «Безопасность автоматизированных систем»).

Общая трудоемкость дисциплины составляет 4 зачетных единиц.

Форма контроля: экзамен.

Предполагаемый семестр: 8.

Целью изучения дисциплины является овладение студентами методами выявления нарушений информационной безопасности.

Задачами курса являются:

- ознакомление с общими принципами работы традиционных механизмов защиты и систем обнаружения атак;
- изучение различных классификаций атак и уязвимостей;
- изучение перечня источников информации об атаках;
- ознакомление с методами обработки и анализа собранной информации об атаках;
- ознакомление с инфраструктурой обнаружения атак;
- ознакомление с проблемами, присущими технологии обнаружения атак и их решениями.

Учебная дисциплина относится к циклу БЗ. Для освоения дисциплины необходимы знания, полученные при изучении следующих дисциплин:

- сети и системы передачи информации;
- безопасность операционных систем;

- безопасность вычислительных сетей
- иностранный язык (английский).

Знания и практические навыки, полученные в результате освоения дисциплины, используются студентами при разработке курсовых и дипломных работ, в научно-исследовательской работе.

Краткое содержание дисциплины:

Традиционные средства защиты информации и их недостатки.

События безопасности и уязвимости.

Классификация атак.

Источники информации об атаках.

Методы обнаружения атак.

Классификация систем обнаружения атак.

Инфраструктура обнаружения атак.

Недостатки технологии обнаружения атак и способы их устранения.

Системы анализа защищенности. Обманные системы. Системы контроля целостности.

Классы потребителей систем обнаружения атак и их требования.

Обоснование для руководства.

Варианты размещения систем обнаружения атак.

Эксплуатация систем обнаружения атак.

Знакомство с системой обнаружения атак RealSecure.

В результате изучения дисциплины, бакалавр должен обладать следующими профессиональными компетенциями (ПК):

эксплуатационная деятельность:

ПК-8: способностью 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;

ПК-10: способностью администрировать подсистемы информационной безопасности объекта;

ПК-11: способностью выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации;

ПК-17: способностью к программной реализации алгоритмов решения типовых задач обеспечения информационной безопасности;

ПК-21: способностью проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов;

ПК-23: способностью принимать участие в проведении экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности;

ПК-24: способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности;

организационно-управленческая деятельность:

ПК-25: способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью;

ПК-30: способностью применять комплексный подход к обеспечению информационной безопасности в различных сферах 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.

Аннотация к рабочей программе дисциплины Б3.В. Мировые информационные ресурсы

Направление подготовки 090900.62 «Информационная безопасность».

Профиль подготовки – «Безопасность автоматизированных систем».

Общая трудоемкость дисциплины составляет 3 зачетных единицы.

Форма контроля: зачет.

Предполагаемые семестры: 6

Цель дисциплины - овладение необходимым минимумом знаний по созданию современных систем обработки информации с использованием мировых информационных ресурсов.

Задачами дисциплины являются:

Освоение принципов создания глобальной информационной сети Интернет, а также структуры адресного пространства.

Изучение систем поиска необходимой информации на региональном и глобальном уровнях.

Разработка персональных сайтов общего.

Учебная дисциплина Мировые информационные ресурсы Б3.В Дисциплина по выбору.

Для освоения дисциплины необходимы знания по дисциплинам математического и естественнонаучного цикла и дисциплин по выбору:

- Операционные системы.
- Базы данных.
- Сети и телекоммуникации.
- Защита информации ЭВМ и периферийные устройства.
- Программирование.
- Информационные технологии.

На основании усвоения дисциплины можно продолжать обучение студента дисциплинам: «Системы искусственного интеллекта», «Технологии программирования», «Теоретические основы автоматизированного управления».

Освоение дисциплины является стадией подготовки бакалавра по направлению «Информационная безопасность».

Краткое содержание дисциплины:

- Раздел 1. История создания компьютерной коммуникационной сети:
- Раздел 2. Потребители информации и поставщики
- Раздел 3. Сервисы Интернет
- Раздел 4. Защита информации в Интернете
- Раздел 5. Поисковые машины и сервера
- Раздел 6. Информация в Интернете
- Раздел 7. Технологии Интернет в бизнесе.
- Раздел 8. Работа в Интернете

- Раздел 9. Создание сайтов
 - **ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ (МОДУЛЯ)**

Выпускник должен обладать следующими **общекультурными компетенциями (ОК):**

способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей её достижения, владеет культурой мышления (ОК-1);

способностью к кооперации с коллегами, работе в коллективе (ОК-3);

способностью находить организационно - управленческие решения в нестандартных ситуациях и готов нести за них ответственность (ОК-4);

способностью к саморазвитию, повышению своей квалификации и мастерства (ОК-6).

Выпускник должен обладать следующими **профессиональными компетенциями (ПК):**

способностью использовать прикладные программные средства при решении практических задач профессиональной деятельности, методы стандартных испытаний по определению физико-механических свойств и технологических показателей материалов и готовых изделий, стандартные методы их проектирования, прогрессивные методы эксплуатации изделий (ПК-4);

способностью участвовать в разработке проектов изделий с учетом технологических, конструкторских, эксплуатационных, эстетических, экономических и управленческих параметров (ПК-8);

способностью использовать современные информационные технологии при проектировании изделий, производств (ПК-10);

способностью выбирать технологии, инструментальные средства и средства вычислительной техники при организации процессов проектирования, изготовления, контроля и испытания продукции, средства и системы автоматизации, контроля, диагностики, испытаний, управления производством, жизненным циклом продукции и ее качеством (ПК-32);

способностью выполнять работу по организации управления информационными потоками на всех этапах жизненного цикла продукции, ее интегрированной логистической поддержки (ПК-33);

способностью организовывать работы по обслуживанию и реинжинирингу бизнес-процессов предприятия в соответствии с требованиями ИПИ/ CALS-технологий, анализе и оценки производственных и непроизводственных затрат на обеспечение требуемого качества продукции, автоматизацию производства, результатов деятельности производственных подразделений, разработке оперативных планов их функционирование (ПК-36);

способностью аккумулировать научно-техническую информацию, отечественный и зарубежный опыт в области автоматизации технологических процессов и производств, автоматизированного управления жизненным циклом продукции, компьютерных систем управления ее качеством (ПК-39);

способностью участвовать в разработке алгоритмического и программного обеспечения средств и систем автоматизации и управления процессами (ПК-41).

В результате изучения дисциплины студенты должны знать:

- основные термины и понятия Интернет;
- принципы построения Интернет;
- поиск информации в локальных и глобальных базах данных;
- защиту информации от несанкционированного доступа;
- перспективы развития поисковых систем.

В результате изучения дисциплины студенты должны уметь:

- производить настройку браузеров Интернет;
- решать задачи по применению поисковых систем Интернет в практической работе;
- оценивать эффективность различных методов поиска информации для бизнеса и индустрии развлечений.

В результате изучения дисциплины студенты должны владеть:

- методами и средствами создания веб страниц в Интернете;
- Созданием веб страниц и сайтов для общего доступа в Интернете;
- Системами поиска информации в Интернете.

Аннотация к рабочей программе

**дисциплины «Моделирование информационной безопасности АС»
по направлению 090900.62 «Информационная безопасность»
(профиль «Безопасность автоматизированных систем»).**

Общая трудоемкость дисциплины составляет 3 зачетные единицы.

Форма контроля: зачет

Предполагаемый семестр: 6.

Цель изучения дисциплины является:

- изучение основных понятий теории моделирования, классификаций видов моделирования, этапов построения моделей на ЭВМ;
- приобретение навыков статистического моделирования и построения кибернетических моделей;
- умение использовать языки моделирования, анализировать полученный результат, знать основные методы моделирования систем, способы разработки и представления имитационных моделей систем.

Имитационное моделирование чрезвычайно важно как предварительный этап процесса принятия решений. Причем современные среды позволяют промоделировать процессы самых разных предметных областей с различным уровнем детализации: системы массового обслуживания, производственные процессы, процессы обработки информации и т.д.

Благодаря появлению различных программных сред и высокопроизводительных компьютерных систем, имитационное моделирование процессов и систем является одним из современных средств моделирования, позволяет проследить за процессом функционирования системы, выявить недостатки, проанализировать, сделать прогнозы, оптимизировать работу системы, в удобном виде представить результаты моделирования.

Задачами курса являются:

- *познакомить студентов с этапами построения моделей, с вопросами*

статистического моделирования систем; оценки точности и достоверности результатов; планированием имитационных экспериментов; формализацией и алгоритмизацией процессов функционирования систем; принципами построения моделирующих алгоритмов; перспективами развития машинного моделирования сложных систем;

- *научить использовать* язык GPSS (General Purpose Simulation System) для построения имитационных моделей процессов и технических объектов, с целью оценки информационной безопасности системы;

- *научить студентов* изучать и использовать дополнительную литературу для самостоятельного освоения других сред моделирования.

Учебная дисциплина «Моделирование информационной безопасности автоматизированных систем» относится к профессиональному циклу (Б2.Б), поскольку является одной из основных компонентов в специализации при профессиональной подготовке.

Знания, полученные по дисциплине «Моделирование информационной безопасности автоматизированных систем», непосредственно используются при изучении дисциплин:

- Моделирование угроз информационной безопасности;
- Технология построения защищенных автоматизированных систем;
- Принципы построения, проектирования и эксплуатации автоматизированных информационных систем;
- Комплексное обеспечение информационной безопасности АС.

Краткое содержание дисциплины:

Основные понятия теории моделирования систем.

Модели оптимизационные и теории игр.

Организация статистического моделирования систем на ЭВМ.

Инструментальные средства реализации моделей. Языки и системы моделирования. Язык моделирования GPSS.

В результате изучения дисциплины, бакалавр должен обладать следующими профессиональными компетенциями (ПК):

В результате изучения дисциплины бакалавр должен обладать следующими профессиональными компетенциями:

ПК-19: способностью составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности;

ПК-20: способностью применять методы анализа изучаемых явлений, процессов и проектных решений;

ПК-21: способностью проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов;

ПК-22: способностью проводить эксперименты по заданной методике, обработку результатов, оценку погрешности и достоверности их результатов;

ПК-23: способностью принимать участие в проведении экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности;

ПК-24: способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам

обеспечения информационной безопасности.

**Аннотация к рабочей программе
Дисциплины «Организационное и правовое обеспечение ИБ»
по направлению 090900.62 Информационная безопасность
(профиль «Безопасность автоматизированных систем»)**

Общая трудоемкость дисциплины составляет 4 зачетных единицы

Форма контроля: экзамен

Предполагаемые семестры: 5.

Цели освоения дисциплины « Организационное и правовое обеспечение ИБ» состоят:

- в изучении способов разработки и реализации мер по организации на предприятиях, государственных учреждениях информационной безопасности;
- в решении задач, требующих классификации и структуризации объектов информационной безопасности от степени конфиденциальности.

Задачами курса является изучение основ организационного и правового обеспечения информационной безопасности; основных нормативных, правовых актов в области обеспечения ИБ и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации; правовых основ организации защиты государственной тайны и конфиденциальной информации, задач органов защиты государственной тайны; организации работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации. Применение нормативных правовых актов и нормативных методических документов в области обеспечения ИБ; разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации.

Учебная дисциплина «Организационное и правовое обеспечение ИБ» входит в профессиональный цикл (базовая часть). Дисциплина является самостоятельным элементом в системе подготовки специалиста, относится к циклу БЗ.Б.11. Для освоения дисциплины необходимы знания, полученные при изучении следующих дисциплин:

- основы информационной безопасности;
- информатика.

В дисциплине «Организационное и правовое обеспечение ИБ» определяются теоретические основы и практические навыки, при освоении которых студент способен приступить к изучению следующих дисциплин в соответствии с учебным планом:

- разработка и эксплуатация защищенных автоматизированных систем;
- информационная безопасность автоматизированных транспортных систем;
- информационная безопасность информационно-управляющих и информационно - логистических систем.

Краткое содержание дисциплины

Актуальность информационной безопасности для организаций. Организация и ведение учета информационных ресурсов. Анализ информационных рисков. Определение правил или политики информационной безопасности в организациях и учреждениях. Контроль или аудит ИБ, оценка уровня ИБ. Организация и обеспечение режима секретности. Организация работы по обеспечению контроля сотрудников организации. Организация охраны объектов.

В результате изучения дисциплины специалист должен обладать следующими профессиональными компетенциями:

ОК-1: способностью осознавать необходимость соблюдения Конституции Российской Федерации, прав и обязанностей гражданина своей страны, гражданского долга и проявления патриотизма.

ОК-2: способностью осуществлять свою деятельность в различных сферах общественной жизни с учетом принятых в обществе моральных и правовых норм;

ОК-5: способностью к кооперации с коллегами, работе в коллективе;

ОК-6: способностью находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность;

ОК-7: способностью осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности, готовностью и способностью к активной созидательной деятельности в условиях информационного противоборства;

ПК-1: способностью использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности;

ПК-2: способностью 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;

ПК-3: способностью использовать нормативные правовые документы в своей профессиональной деятельности.

ПК-4: способностью формировать комплекс мер по информационной безопасности с учетом 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 учетом 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;

ПК-11: способностью выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации.

ПК-14: способностью оформить рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности.

ПК-19: способностью составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности.

ПК-24: способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности.

ПК-25: способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью.

ПК-26: способностью формировать комплекс мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью.

ПК-31: способностью организовать работу малого коллектива исполнителей с учетом требований защиты информации.

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

**Аннотация к рабочей программе дисциплины
«Организация работы администратора автоматизированных систем»
по направлению 090900.62 «Информационная безопасность»
(профиль «Безопасность автоматизированных систем»).**

Общая трудоемкость дисциплины составляет 4 зачетных единиц.

Форма контроля: экзамен.

Предполагаемый семестр: 8.

Целью изучения дисциплины (модуля) является овладение студентами методами администрирования и поддержки сетей Windows Server 2008.

Задачами курса являются:

- ознакомление с общими сведениями о TCP/IP;
- изучение преимуществ и возможностей протокола DHCP;
- изучение основных параметров конфигурирования DNS-серверов и зон;
- изучение основных параметров настройки маршрутизации.

Учебная дисциплина относится к циклу БЗ. Для освоения дисциплины необходимы знания, полученные при изучении следующих дисциплин:

- сети и системы передачи информации;
- безопасность операционных систем;
- безопасность вычислительных сетей
- иностранный язык (английский).

Знания и практические навыки, полученные в результате освоения дисциплины, используются студентами при разработке курсовых и дипломных работ, в научно-исследовательской работе.

Краткое содержание дисциплины:

Уровни и модели TCP/IP. IP-адресация. Разбиение IP-сетей на подсети и создание надсетей. Установка и конфигурирование TCP/IP на примере Windows Server 2008.

Анализ сетевого трафика средствами «Сетевого монитора». Устранение неполадок подключений TCP/IP.

Сравнение DNS и NetBIOS. DNS в сетях Windows Server 2008. Развертывание DNS-серверов. Настройка DNS-клиентов. Настройка параметров DNS-сервера. Настройка свойств зоны и передачи. Настройка дополнительных свойств DNS-сервера.

Средства устранения неполадок DNS. Средства мониторинга DNS.

Настройка DHCP-сервера. Управление DHCP в сетях Windows.

Анализ DHCP-трафика. Мониторинг DHCP с применением журнала аудита. Устранение неполадок DHCP.

Настройка Windows Server 2008 для маршрутизации в локальной сети. Настройка маршрутизации вызовов по требованию.

Настройка преобразования сетевых адресов (NAT). Настройка и управление протоколами маршрутизации. Настройка фильтров пакетов.

В результате изучения дисциплины, бакалавр должен обладать следующими профессиональными компетенциями (ПК):

эксплуатационная деятельность:

ПК-8: способностью 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;

ПК-9: способностью принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия;

ПК-10: способностью администрировать подсистемы информационной безопасности объекта;

ПК-11: способностью выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации;

ПК-17: способностью к программной реализации алгоритмов решения типовых задач обеспечения информационной безопасности;

ПК-21: способностью проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов.

Аннотация к рабочей программе дисциплины «Основы кибернетики»

по направлению 090900.62 «Информационная безопасность»

(профиль «Безопасность автоматизированных систем»).

Общая трудоемкость дисциплины составляет 4 зачетные единицы.

Форма контроля: зачет

Предполагаемый семестр: 4.

Целью изучения дисциплины является формирование у студентов способности при решении профессиональных задач уметь анализировать предметную область и процессы с применением методов системного анализа, логики, ставить и решать задачи кибернетики с использованием современных информационно-коммуникационных технологий.

Содержание курса содержит обзор моделей, методов и алгоритмов решений задач кибернетики, а также возможности использования пакетов прикладных программ. В теоретической части курса дается представление функций алгебр логики с помощью таблиц и ДНФ, рассматриваются алгоритмы минимизации ДНФ, рассматривается описание структуры и функционирование схем из основных классов управляющих систем, изучаются эквивалентные преобразования схем на основе тождеств, изучаются вопросы полноты и избыточности, рассматривается задача синтеза управляющих систем. На практических занятиях студенты отрабатывают навыки формализации задачи, построения моделей.

Задачами курса являются:

- изучение основных видов дискретных математических моделей, описывающих функционирование и структуру сложных систем преобразования информации (интегральных схем, программ и т.д.), алгоритмы и методы их реализации;

- умение формализовать задачу, использовать готовые алгоритмы решения, выбирать нужное решение из множества по некоторому критерию оптимальности, уметь оценивать сложность системы;

- овладение навыками минимизации ДНФ, эквивалентных преобразований схем, методами синтеза управляющих систем.

Учебная дисциплина «Основы кибернетики» относится к циклу дисциплины по выбору (Б2.ДВ2).

Знания, полученные по дисциплине «Основы кибернетики», непосредственно используются при изучении дисциплин:

- Схемотехника;
- Технология построения защищенных автоматизированных систем.

Краткое содержание дисциплины:

Введение в кибернетику.

Кибернетика как наука об информации и искусство управления. Основные понятия теории информации и управления, кодирование информации.

Представление функций алгебры логики с помощью ДНФ, минимизация ДНФ.

Тупиковая ДНФ. Ядро и ДНФ ФАЛ. Таблицы Квайна. Пересечение тупиковых ДНФ. Задача контроля схем и построение тестов для таблиц.

Основные классы управляющих систем. Эквивалентные преобразования управляющих систем. Логические формулы, их структура. Эквивалентность формул.

Задачи синтеза УС. Простейшие методы синтеза УС. Оценки сложности. Метод каскадов, метод Шеннона.

В результате изучения дисциплины, бакалавр должен обладать следующими общекультурными (ОК) и профессиональными компетенциями (ПК):

способностью к кооперации с коллегами, работе в коллективе (ОК-5);

способностью находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность (ОК-6);

способностью осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности, готовностью и способностью к активной созидательной деятельности в условиях информационного противоборства (ОК-7);

способностью критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков (ОК-12);

способностью использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности (ПК-1);

способностью 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 (ПК-2);

способностью применять программные средства системного, прикладного и специального назначения (ПК-15).

Аннотация

к рабочей программе учебной дисциплины

«Основы управленческой деятельностью»

по направлению 090900.62 Информационная безопасность

(профиль «Безопасность автоматизированных систем»)

Общая трудоемкость дисциплины составляет 3 зачетных единиц.

Форма контроля: зачет

Предполагаемые семестры: 3

Целями освоения учебной дисциплины (модуля) сформировать у студентов знания и навыки по управлению различными видами деятельности, обеспечивающие компаниям более высокую рентабельность.

Задачами курса являются: дать студентам необходимые знания, умения и навыки, в том числе: теоретические и практические проблемы управления в бизнесе; навыки самостоятельного, творческого использования теоретических знаний в практической деятельности управленца.

Дисциплина относится к циклу Б1.Б. Для освоения дисциплины необходимы знания, полученные при изучении следующих дисциплин:

- Математика. Математический анализ;
- Информатика;
- Математическая логика и теория алгоритмов.
- Документоведение;
- Основы системного анализа;
- Основы информационной безопасности;

В дисциплине «Основы управленческой деятельности» определяются теоретические основы и практические навыки, при освоении которых студент способен приступить к изучению следующих дисциплин в соответствии с учебным планом:

- Вычислительная математика и численные методы;
- Математические основы прогнозирования.

Краткое содержание дисциплины:

Управление, как основа деятельности предприятий.

Управление кадрами и деятельностью коллектива.

Управленческие решения.

Коммуникации в управлении организацией.

В результате изучения дисциплины бакалавр должен обладать следующими профессиональными компетенциями:

ОК-5: способностью к кооперации с коллегами, работе в коллективе;

ОК-6: способностью находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность;

ОК-7: способностью осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности, готовностью и способностью к активной созыательной деятельности в условиях информационного противоборства;

ОК-12: способность критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков;

ПК-4: способностью формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности;

ПК-5: способностью организовывать проведение и поддерживать процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации;

ПК-7: способностью использовать основные методы защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий;

ПК-8: способностью 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;

ПК-25: способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью;

ПК-26: способностью формировать комплекс мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью;

ПК-31: способностью организовать работу малого коллектива исполнителей с учетом требований защиты информации.

**Аннотация к рабочей программе
дисциплины «Правоведение»
по направлению 090900.62 Информационная безопасность
(профиль «Безопасность автоматизированных систем»).**

Общая трудоемкость дисциплины составляет 3 зачетных единиц.

Форма контроля: зачет.

Предполагаемые семестры: 4.

Целями освоения учебной дисциплины являются: является изучение и в дальнейшем умение применить полученные знания в области правоведения на практике, в повседневной жизни.

Задачами курса являются: формирование целостного представления об основных особенностях правовой системы российского государства и системы российского права, обучение приемам и принципам законодательной базы РФ и их использованию в профессиональной деятельности.

Учебная дисциплина «Правоведение» входит в гуманитарный, социальный, экономический цикл (базовая часть) и относится к числу фундаментальных юридических дисциплин, поскольку служит основой для изучения учебных дисциплин правового цикла.

Знания, полученные по дисциплине «Правоведение», непосредственно используются при изучении дисциплин базового цикла:

- «Основы трудового права»;
- «Предпринимательское право»;
- «Хозяйственное право».

Краткое содержание дисциплины:

Основы теории государства и права

Основы конституционного права

Основы гражданского права

Основы административного права

Основы трудового права

Основы семейного права

Основы уголовного права

Основы экологического права

Основы информационного права.

В результате изучения дисциплины бакалавр должен обладать следующими профессиональными компетенциями:

ОК-1: способен осознавать необходимость соблюдения Конституции Российской Федерации, прав и обязанностей гражданина своей страны, гражданского долга и проявления патриотизма;

ОК-2: способен осуществлять свою деятельность в различных сферах общественной жизни с учетом принятых в обществе моральных и правовых норм;

ОК-4: способен 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;

ОК-7: способен осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к профессиональной деятельности в области обеспечения информационной безопасности, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства;

ОК-11: способен к саморазвитию, самореализации, приобретению новых знаний повышению своей квалификации и мастерства;

ПК-3: способен использовать нормативные правовые документы в своей профессиональной деятельности;

ПК-4: способен формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности;

ПК-7: способен использовать основные методы защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий;

ПК-14: способен оформить рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности;

ПК-24: способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности;

ПК-33: способен организовывать технологический процесс защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности РФ, Федеральной службой по техническому и экспортному контролю.

**Аннотация к рабочей программе дисциплины
«Принципы построения, проектирования и эксплуатации
автоматизированных информационных систем»
по направлению 090900.62 «Информационная безопасность»
(Профиль «Безопасность автоматизированных систем»)**

Общая трудоемкость дисциплины составляет 5 зачетных единиц.

Форма контроля: экзамен.

Предполагаемый семестр: 6.

Цели освоения дисциплины «Безопасность вычислительных сетей» состоят:

– в получении знаний и навыков работы, необходимых для разработки и эксплуатации автоматизированных систем.

– в изучении принципов построения информационных систем и принципов организации информационных систем в соответствии с требованиями по защите информации.

Задачами курса являются:

– изучение принципов построения информационных систем;
– освоение принципов организации информационных систем в соответствии с требованиями по защите информации;

– ознакомление с основными нормативно-правовыми актами в области информационной безопасности и защиты, а также нормативно-методическими документами Федеральной службы безопасности Российской Федерации.

Дисциплина является самостоятельным элементом в системе подготовки специалиста, относится к циклу БЗ.В.2. Для освоения дисциплины необходимы знания, полученные при изучении следующих дисциплин:

– основы информационной безопасности;
– принципы построения, проектирования и эксплуатации автоматизированных информационных систем.

В дисциплине «Безопасность вычислительных сетей» определяются теоретические основы и практические навыки, при освоении которых студент способен приступить к изучению следующих дисциплин в соответствии с учебным планом:

– комплексное обеспечение информационной безопасности автоматизированных систем;
– интегрированные информационные системы в управлении.

Краткое содержание дисциплины:

Стадии и этапы создания автоматизированных информационных систем (АИС).

Исследование и формализация бизнес-процессов деятельности.

Модели информационного пространства предприятия.

Автоматизация документооборота

Технология создания распределенных АИС.

В результате изучения дисциплины, бакалавр должен обладать следующими компетенциями:

ОК-5: способностью к кооперации с коллегами, работе в коллективе;

ОК-6: способностью находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность;

ОК-7: способностью осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности, готовностью и способностью к активной созидательной деятельности в условиях информационного противоборства.

ОК-8: способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления;

ОК-9: способностью логически верно, аргументировано и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии.

ПК-25: способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью.

ПК-26: способностью формировать комплекс мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью.

ПК-27: способностью принимать участие в организации контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации.

ПК-28: способностью изучать и обобщать опыт работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации.

ПК-29: способностью участвовать в работах по реализации политики информационной безопасности.

ПК-30: способностью применять комплексный подход к обеспечению информационной безопасности в различных сферах деятельности.

ПК-31: способностью организовать работу малого коллектива исполнителей с учетом требований защиты информации.

ПК-32: способностью организовать мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств защиты информации.

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.

Аннотация к рабочей программе
дисциплины «Программно-аппаратные средства защиты
информации»
по направлению 090900.62 «Информационная безопасность»
(профиль «Безопасность автоматизированных систем»).

Общая трудоемкость дисциплины составляет 4 зачетные единицы.

Форма контроля: экзамен.

Предполагаемые семестры: 7.

Целями освоения учебной дисциплины являются: обучение принципам построения систем защиты информации (СЗИ) в операционных системах, на рабочих станциях и персональных компьютерах (РС), в вычислительных сетях (ВС) и системах управления базами данных (СУБД).

Задачами курса являются: изучение основ построения подсистем защиты информации в автоматизированных системах различной архитектуры; освоение принципов функционирования современных систем идентификации и аутентификации; изучение принципов построения и использования межсетевых экранов (МЭ); изучение основ построения систем безопасности в вычислительных

сетях.

Учебная дисциплина «Программно-аппаратные средства защиты информации» входит в профессиональный цикл (базовая часть).

Знания, полученные при изучении дисциплины «Программно-аппаратные средства защиты информации», непосредственно используются при изучении дисциплин профессионального цикла:

- «Комплексное обеспечение информационной безопасности автоматизированных систем»;
- «Методы выявления нарушений информационной безопасности»;
- «Интегрированные информационные системы в управлении».

Краткое содержание дисциплины:

Группы методов и средств программно-аппаратной защиты информации.

Идентификация и аутентификация. Электронная цифровая подпись.

Защита от удаленных атак через глобальные сети.

Антивирусная защита.

Защищенные программно-аппаратные комплексы.

В результате изучения дисциплины бакалавр должен обладать следующими профессиональными компетенциями:

обще профессиональными:

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 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;

эксплуатационная деятельность:

ПК-9: способностью принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия;

ПК-11: способностью выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации;

проектно-технологическая деятельность:

ПК-12: способностью участвовать в разработке подсистем управления информационной безопасностью;

ПК-15: способностью применять программные средства системного, прикладного и специального назначения;

ПК-16: способностью использовать инструментальные средства и системы программирования для решения профессиональных задач;

ПК-17: способностью к программной реализации алгоритмов решения типовых задач обеспечения информационной безопасности;

ПК-18: способностью собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности;

экспериментально-исследовательская деятельность:

ПК-21: способностью проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов;

ПК-22: способностью проводить эксперименты по заданной методике, обработку результатов, оценку погрешности и достоверности их результатов;

организационно-управленческая деятельность:

ПК-27: способностью принимать участие в организации контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации;

ПК-28: способностью изучать и обобщать опыт работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации.

АННОТАЦИЯ ДИСЦИПЛИНЫ

«Русский язык и культура речи»

Для направления подготовки 090900 Информационная безопасность

Профиль Безопасность автоматизированных систем

Общая трудоемкость дисциплины составляет 2 зачетных единиц.

Форма контроля: зачет.

Предполагаемые семестры: 1.

Дисциплина «Русский язык и культура речи» относится к вариативной части цикла ГСЭ и является гуманитарной и общепрофессиональной основой системы подготовки бакалавров. Данная дисциплина имеет самостоятельное значение и направлена на формирование необходимых специалисту логической основы мышления, мировоззрения, соответствующих ценностных ориентаций и идеалов.

Курс «Русский язык и культура речи» (для нефилологов) нацелен на повышение уровня практического владения современным русским литературным языком у специалистов нефилологического профиля – в разных сферах функционирования русского языка, в письменной и устной его разновидностях. Овладение новыми навыками и знаниями в этой области и совершенствование имеющихся неотделимо от углубления понимания основных характерных свойств русского языка как средства общения и передачи информации, а также расширения общепрофессионального кругозора, опирающегося на владение богатым коммуникативным, познавательным и эстетическим потенциалом русского языка.

Цель курса – формирование у студентов общей, коммуникативной и профессиональной компетенции. Общая компетенция предполагает развитие у студентов способностей и навыков к социальному взаимодействию; коммуникативная и профессиональная компетенция направлена на формирование умений и навыков

соотносить языковые средства с конкретными сферами, ситуациями, условиями и задачами общения, включая деловую сферу общения.

Задачи курса состоят в формировании у студентов следующих основных навыков, которые должен иметь профессионал любого профиля для успешной работы по своей специальности и каждый член общества – для успешной коммуникации в самых различных сферах – научной, политической, социально-государственной, бытовой, юридически-правовой:

1. продуцирование связных, правильно построенных монологических текстов на разные темы в соответствии с коммуникативными намерениями говорящего и профессиональной ситуацией общения;

2. участие в диалогических и полилогических ситуациях общения, установление речевого контакта, обмен информацией с другими членами языкового коллектива, связанными с говорящим различными социальными отношениями;

3. формирование навыков и умений речевой деятельности применительно к сфере научной и профессиональной коммуникации, основам публичной речи, владение нормами официально-деловой письменной речи: составление частной документации (заявление, резюме, доверенности, расписки); ведение деловой переписки (составление делового письма); составление информационно-справочных документов (протокол, план, справка, докладная, отчет);

4. Развитие у студентов умения понимать текст, ориентированный на ту или иную форму речевого общения; а также владения навыками самостоятельного порождения стилистически мотивированного текста;

5. Совершенствование навыков реферирования и аннотирования литературы по специальности.

В ходе изучения курса «Русский язык и культура речи» студенты должны не просто укрепить знания в перечисленных областях, но научиться практически применять их для построения текстов, продуктивного участия в процессе общения, достижения своих коммуникативных целей.

В соответствии с требованиями ГОС третьего поколения при реализации компетентностного подхода (пункт 7.3) изучение дисциплины предусматривает использование интерактивных форм проведения занятий (деловых и ролевых игр, лингвистических тренингов), рейтинговую оценку освоения дисциплины, обращение к интернет-ресурсам по культуре речи и деловому общению.

Полностью сформирована учебно-информационная база по данной дисциплине: учебная литература, которая в достаточном количестве имеется в библиотеке ФГОУ ВПО СибАДИ: Введенская Л.А и др. Русский язык и культура речи. Ростов-на-Дону, 2008 (500 экз.); Кобзеева О.В. Русский язык и культура речи: Учебное пособие Учебное пособие. – Омск: Изд-во СибАДИ, 2008. (300 экз.); Кобзеева О.В., Ким Ю.Н. Особенности официально-деловой письменной речи: Учебное пособие. – Омск: Изд-во СибАДИ, 2009. (100 экз.) и др., а также на кафедре имеются все необходимые лингвистические словари и технические средства.

В результате освоения дисциплины студент должен

знать:

– основные нормы современного русского литературного языка (нормы словоупотребления, нормы русской грамматики, орфографические и пунктуационные нормы);

- основные нормы культуры речи;
- нормы деловой речи.

уметь:

- логически верно аргументировать и доказывать, опираясь на современные научные данные;
- стремиться к саморазвитию, повышению своей квалификации и мастерства;
- вести научную и профессиональную коммуникацию на государственном языке;
- понимать тексты различных жанров в профессионально-ориентированной коммуникации;
- создавать все виды устной и письменной деловой документации.

владеть:

- основами реферирования и аннотирования литературы по специальности;
- навыками составления научных и профессиональных текстов различных жанров;
- культурой мышления, способностью к обобщению, анализу, восприятию информации, постановке цели и выборе путей ее достижения;
- способностью вести культурный диалог с различными социокультурными группами;
- навыками абсолютно грамотного письма.

Процесс изучения дисциплины направлен на формирование следующих общекультурных компетенций выпускника ОК-8, ОК-9.

Общая трудоемкость дисциплины составляет 3 зачетных единиц. В конце семестра по дисциплине предусмотрен зачет.

Краткое содержание дисциплины:

1. Язык как средство общения. Язык и речь. Виды речевой деятельности. Понятие о культуре речи.
2. Нормы языка. Основные типы норм. Система правил орфографии и пунктуации как нормы письменной речи.
3. Научный текст. Сферы функционирования, языковые особенности. Жанровые и структурные особенности, подстили, первичные и вторичные жанры.
4. Официально-деловой стиль. Язык и стиль основных типов документов. Унификация языка деловых бумаг. Новые тенденции в практике русского делового письма. Требования к речевой коммуникации в деловой среде. Факторы успеха в проведении делового совещания. Мозговой штурм. Телефонный этикет.
5. Деловое общение. Речевые коммуникации в деловых переговорах. Культура ораторской речи в деловом стиле.
6. Основные особенности публицистического стиля.
7. Основы классической риторики. Речевое общение и ораторское искусство. Подготовка речи: выбор темы, цель речи. Логические уловки в споре.
8. Основные особенности разговорно-бытового стиля.
9. Речевой этикет.

Разработчик:

Доцент кафедры иностранных языков,
кандидат филологических наук О.В. Кобзеева.

**Аннотация к рабочей программе
дисциплины «Сети и системы передачи информации»
по направлению подготовки 090900.62 «Информационная безопасность»
(Профиль «Безопасность автоматизированных систем»)**

Общая трудоемкость дисциплины составляет 4 зачетных единиц

Форма контроля: экзамен

Предполагаемые семестры: 5

Целями освоения дисциплины «Сети и системы передачи информации» являются:

- получение системного представления о современных сетях передачи информации;
- приобретение знаний об основных видах систем передачи данных и их характеристик, о характере формирования сигналов, способах их обработки;
- формирование навыков по построению современных сетевых топологий и систем связи, использованию перспективных технологий, стандартов и протоколов передачи данных.

Учебная дисциплина «Сети и системы передачи информации» входит в профессиональный цикл (базовая часть).

Знания, полученные по дисциплине, непосредственно используются студентами при разработке курсовых и дипломных работ, в научно-исследовательской работе и для изучения следующих базовых дисциплин:

- программно-аппаратные средства обеспечения информационной безопасности;
- разработка и эксплуатация защищенных автоматизированных систем.

Краткое содержание дисциплины

Классификация систем и линий связи. Кодирование информации в системах связи. Методы и алгоритмы сжатия информации. Цифровая обработка сигналов. Шифрование информации в системах связи. Спецификация, характеристики и протоколы систем связи.

Организация передачи данных по вычислительным сетям. Эталонная модель взаимодействия открытых систем. Стеки протоколов вычислительных сетей. Сетевые архитектуры систем связи. Технологии высокоскоростной передачи данных в глобальных сетях. Базовые стандарты технологии беспроводных сетей. Протоколы межсетевое взаимодействия. Диагностика локальных сетей и Интернет.

В результате изучения дисциплины бакалавр должен обладать следующими профессиональными компетенциями:

ПК-1 способностью использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности.

ПК-2: способностью 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.

ПК-8: способностью 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.

ПК-11: способностью выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации.

ПК-22: способностью проводить эксперименты по заданной методике, обработку результатов, оценку погрешности и достоверности их результатов.

ПК-23: способностью принимать участие в проведении экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности.

Аннотации

**к рабочей программе дисциплины «Случайные процессы»
по направлению 090900.62 «Информационная безопасность»**

(профиль «Безопасность автоматизированных систем»)

Общая трудоемкость дисциплины составляет 3 зачетные единицы.

Форма контроля: зачет

Предполагаемые семестры: 6.

Цель освоения учебной дисциплины:

Курс « Случайные процессы» является базой для конструирования алгоритмов по идентификации внутренних и внешних угроз информационной безопасности систем организационного управления в системе подготовки специалиста по ИБ.

Задачами курса являются:

- изучение базовых положений теории случайных процессов;
- приобретение навыков решения задач по нахождению корреляционных функций и спектральных плотностей случайных процессов;
- знакомство с базовыми алгоритмами обнаружения и распознавания образов.

Учебная дисциплина «Случайные процессы» в основной образовательной программе подготовки специалиста находится в блоке математических и естественнонаучных дисциплин. Для успешного усвоения дисциплины необходимо, чтобы студент владел знаниями, умениями, навыками, полученными в процессе изучения курсов «Математический анализ», «Теория вероятностей и математическая статистика», «Языки программирования». Знание случайных процессов используется при изучении курса «Информационно-аналитическая работа по обеспечению информационной безопасностью АС», «Основы прогнозирования».

Знания и практические навыки, полученные из дисциплины «Случайные процессы», используются обучаемыми при разработке курсовых и дипломных работ, в научно-исследовательской работе.

Краткое содержание дисциплины:

Элементы теории случайных процессов.

Понятие СП. Плотность распределения вероятностей СП. Характеристики СП.

Классификация СП. Импульсные. Особенности анализа нестационарных СП.

Линейные преобразования СП (суммирование, дифференцирование,

интегрирование). Нелинейные преобразования СП.

Пуассоновский случайный процесс для описания работы систем массового обслуживания.

Применение теории СП в задачах защиты и обработки информации.

Системы организационного управления АСУ ТП.

Понятие сигнала и шума. Стратегии выделения сигнала на фоне помех.

Анализ эффективности стратегий.

Понятие о разладке случайных процессов. Алгоритмы обнаружения разладки.

Рекомендации по выбору алгоритмов.

Прогнозирование поведения систем. Алгоритм Брауна. Пример использования.

Теория массового обслуживания. Модели сигналов.

Применение теории для решения задач противоборства, включая информационные войны.

В результате изучения дисциплины выпускник должен обладать следующими общекультурными (ОК) и профессиональными компетенциями (ПК):

ОК-8: способность к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления.

ОК-9: способность логически верно, аргументировано и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии.

ОК- 11: способностью к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства.

ОК- 12: способность критически оценивать свои достоинства и недостатки.

ПК-1: способность использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности;

ПК-21: способностью проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов.

**Аннотация к рабочей программе
дисциплины «Системы управления базами
данных»**

**по направлению подготовки 090900.62 «Информационная безопасность»
(профиль подготовки «Безопасность автоматизированных систем»)**

Общая трудоемкость дисциплины составляет 5 зачетных единиц.

Форма контроля: зачет, экзамен.

Предполагаемые семестры: 6, 7.

Целями курса являются формирование представлений о архитектурах современных СУБД, особенностях работы с базами данных в сети, о проектировании клиентсерверных приложений, в основе которых используются реляционные, объектно-ориентированные, XML базы данных под управлением современных СУБД. Кроме того,

ставится целью привитие навыков программирования и работы с MS SQL Server 2008 и Oracle Database 10g. Дисциплина является дополнением курса «Безопасность систем баз данных».

Задачами курса являются формирования целостного представления об основных этапах жизненного цикла баз данных и формирование следующих представлений и знаний: закрепление навыков использования стандарта SQL 3; понимание архитектурных особенностей СУБД; знание механизмов импорта/ экспорта данных между СУБД; особенности разработки сетевых приложений для работы с базами данных.

Учебная дисциплина «Системы управления базами данных» относится к профессиональному циклу (БЗ.Б), поскольку является одной из компонент в специализации при профессиональной подготовке.

Знания, полученные по дисциплине «Базы данных», непосредственно используются при изучении дисциплин:

- «Сети и системы передачи информации»;
- «Технология построения защищенных автоматизированных систем»;
- «Принципы построения, проектирования и эксплуатации автоматизированных информационных систем»;
- «Комплексное обеспечение информационной безопасности автоматизированных систем».

Краткое содержание дисциплины:

Понятие СУБД, основные характеристики, функции СУБД.

Планирование работы с СУБД и установка.

SQL стандарт.

Обеспечение сущностной и ссылочной целостности данных.

Представления, курсоры.

Работа с БД в сети, механизм транзакций и блокировок.

Процедуры, функции.

Триггеры.

Распределенные БД, механизм репликаций.

Функции администратора БД.

Поддержание высокой готовности.

Мониторинг производительности СУБД.

Оптимизация запросов.

Анализ объекта автоматизации по заданной предметной области.

Постановка задачи на проектирование базы данных и клиентского интерфейса.

Разработка структуры базы данных по заданной предметной области.

Разработка клиент-серверного приложения в выбранной СУБД и среды программирования.

Разработка сопроводительной документации на установку и эксплуатацию разработанной базы данных и клиентского интерфейса.

В результате изучения дисциплины выпускник должен обладать следующими профессиональными компетенциями (ПК):

ОК-2: способностью осуществлять свою деятельность в различных сферах общественной жизни с учетом принятых в обществе моральных и правовых норм;

ОК-5: способностью к кооперации с коллегами, работе в коллективе;

ОК-6: способностью находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность;

ОК-7: способностью 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;

ОК-8: способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления;

ОК-9: способностью логически верно, аргументированно и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии;

ПК-1: способностью использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности;

ПК-3: способностью использовать нормативные правовые документы в своей профессиональной деятельности;

ПК-4: способностью формировать комплекс мер по информационной безопасности с учетом 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 учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации;

ПК-8: способностью 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;

ПК-11: способностью выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации;

ПК-13: способностью к проведению предварительного технико-экономического анализа и обоснования проектных решений по обеспечению ИБ;

ПК-15: способностью применять программные средства системного, прикладного и специального назначения .

Аннотация к рабочей программе
по дисциплине БЗ.ДВ.1 «Теоретические основы компьютерной
безопасности»

Направление подготовки 090900.62 «Информационная безопасность»

(Профиль «Безопасность автоматизированных систем»)

Общая трудоёмкость дисциплины составляет 180/5 час./ зачетных единиц.

Предполагаемые семестры: 6.

Форма контроля: экзамен 6 семестр

Целями освоения учебной дисциплины являются: получение студентами комплекса знаний о теоретических основах эффективных методов защиты информации и обеспечения компьютерной безопасности, проектирования, разработки и анализа защищённых АС, содействие формированию научного мировоззрения и развитию системного мышления.

Задачами дисциплины являются: формирование целостного представления об устройстве и принципах функционирования защищённых АС, методологии проектирования и построения защищённых АС, критериев и методов оценки защищённости АС, средств и методов реализации несанкционированного доступа (НСД) к информации в АС.

Учебная дисциплина «Теоретические основы компьютерной безопасности» относится к циклу СЗ. Для освоения дисциплины необходимы знания, полученные при изучении следующих дисциплин:

- «Организация ЭВМ и вычислительных сетей»;
- «Технические средства информатизации»;
- «Информационные системы»;
- «Безопасность систем баз данных»;
- «Безопасность операционных систем»;
- «Технологии и методы программирования»;
- "Теория информации";
- "Теория автоматов".

В дисциплине «Теоретические основы компьютерной безопасности» определяются теоретические основы и практические навыки, при освоении которых студент способен приступить к изучению следующих дисциплин в соответствии с учебным планом:

- программно-аппаратные средства обеспечения информационной безопасности;
- криптографические методы защиты информации;
- безопасность вычислительных сетей;
- организационное обеспечение информационной безопасности;
- технология построения защищённых автоматизированных систем.

Краткое содержание дисциплины:

Структура теории компьютерной безопасности.

Методология построения систем защиты АС.

Политика безопасности.

Модели безопасности.

Основные критерии защищенности АС. Классы защищенности АС.

В результате изучения дисциплины бакалавр должен обладать следующими профессиональными компетенциями (ПК):

общекультурными:

ОК-5: способностью к кооперации с коллегами, работе в коллективе;

ОК-6: способностью находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность;

ОК-7: способностью осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности, готовностью и способностью к активной созидательной деятельности в условиях информационного противоборства;

ОК-8: способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления;

ОК-9: способностью логически верно, аргументированно и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии;

профессиональными:

ПК-25: способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью;

ПК-26: способностью формировать комплекс мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью;

ПК-27: способностью принимать участие в организации контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации;

ПК-28: способностью изучать и обобщать опыт работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации;

ПК-29: способностью участвовать в работах по реализации политики информационной безопасности;

ПК-30: способностью применять комплексный подход к обеспечению информационной безопасности в различных сферах деятельности;

ПК-31: способностью организовать работу малого коллектива исполнителей с учетом требований защиты информации;

ПК-32: способностью организовать мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств защиты информации;

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.

Аннотация
рабочей программы учебной дисциплины "Теория вероятностей и
математическая статистика"

по направлению 090900.62 Информационная безопасность
(профиль "Безопасность автоматизированных систем").

Общая трудоемкость дисциплины составляет 4 зачетные единицы.

Форма контроля: экзамен, зачет.

Предполагаемые семестры: 5,6.

Целью освоения учебной дисциплины является формирование у будущего специалиста теоретических знаний и практических навыков по применению теории вероятностей, математической статистики и случайных процессов для решения технических задач.

Задачами курса являются: приобретение навыков практического решения вероятностных задач, обучение приемам и методам статистической обработки экспериментальных данных и формулировке обоснованных выводов по результатам этой обработки; обеспечение возможности изучения в дальнейшем курсов, опирающихся на методы теории вероятностей и математической статистики.

Учебная дисциплина "Теория вероятностей и математическая статистика" входит в математический и естественнонаучный цикл (базовая часть) и относится к числу фундаментальных дисциплин, поскольку служит основой для изучения учебных дисциплин как математического и естественнонаучного, так и профессионального цикла.

Знания, полученные по дисциплине "Теория вероятностей и математическая статистика", непосредственно используются при изучении дисциплины базового цикла:

- Случайные процессы;
- и дисциплин профессионального цикла:
- Криптографические методы защиты информации;
- Основы прогнозирования

В результате изучения дисциплины специалист должен обладать следующими общекультурными и профессиональными компетенциями:

Краткое содержание дисциплины:

Первоначальные понятия теории вероятностей.

Случайные события.

Случайные величины.

Системы случайных величин.

Предельные теоремы теории вероятностей.

Основы математической статистики.

ОК-9: способность логически верно, аргументировано и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии;

ОК-12: способность критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков;

ПК-1: способность использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности;

ПК-2: 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;

ПК-13: способность к проведению предварительного технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности;

ПК-17: способность к программной реализации алгоритмов решения типовых задач обеспечения информационной безопасности;

ПК-18: способность собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности;

ПК-19: способность составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности;

ПК-20: способность применять методы анализа изучаемых явлений, процессов и проектных решений;

ПК-22: способность проводить эксперименты по заданной методике, обработку результатов, оценку погрешности и достоверности их результатов;

ПК-24: способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности

**Аннотация к рабочей программе
дисциплины «Теория информации»
по направлению 090900.62 «Информационная безопасность»
(профиль подготовки «Безопасность АС»)**

Общая трудоемкость дисциплины составляет 3 зачетные единицы.

Форма контроля: зачет.

Предполагаемые семестры: 5.

Целью освоения учебной дисциплины является: обучить студентов принципам построения и анализа математических моделей процессов создания, обработки и передачи информации. Дисциплина обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом, содействует фундаментализации образования, формированию мировоззрения и теоретико-информационного подхода к решению различных прикладных задач, является одной из базовых дисциплин для изучения методов защиты компьютерной информации.

Задачи дисциплины дать основы:

- методов оценки количества информации;
- построения и анализа моделей источников и каналов передачи информации;
- методов оптимального кодирования источников информации и помехоустойчивого кодирования каналов связи.

Учебная дисциплина «Теория информации» входит в математический и естественнонаучный цикл (базовая часть) Изучение дисциплины базируется на дисциплинах: «Математика», «Дискретная математика», «Теория вероятностей и математическая статистика».

Знания и практические навыки, полученные из дисциплины «Теория информации», используются при изучении дисциплин:

- «Криптографические методы защиты информации»;
- «Информационно-аналитические системы»;
- «Информационно-аналитическая работа по обеспечению информационной безопасности АС».

Краткое содержание дисциплины:

Предмет и задачи теории информации. Количество информации и энтропия.

Префиксные коды. Не префиксные коды.

Математические модели каналов связи.

Расстояние Хэмминга между кодовыми словами. Линейные и групповые коды

Совершенные и квазисовершенные коды. Полиномиальные коды.

В результате изучения дисциплины «Теория информации» выпускник должен обладать следующими профессиональными компетенциями (ПК):
общекультурными (ОК):

ОК-9: способностью логически верно, аргументировано и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии;

ОК-12: способностью критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков;

профессиональными (ПК):

общепрофессиональными:

ПК-1: способностью использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности;

ПК-2: способностью 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;

ПК-8: способностью 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;

проектно-технологическая деятельность:

ПК-13: способностью к проведению предварительного технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности;

ПК-17: способностью к программной реализации алгоритмов решения типовых задач обеспечения информационной безопасности;

ПК-18: способностью собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности;

экспериментально-исследовательская деятельность:

ПК-19: способностью составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности;

ПК-20: способностью применять методы анализа изучаемых явлений, процессов и проектных решений;

ПК-22: способностью проводить эксперименты по заданной методике, обработку результатов, оценку погрешности и достоверности их результатов;

ПК-24: способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности.

**Аннотация к рабочей программе
дисциплины «Техническая защита информации»
по направлению 090900.62 «Информационная безопасность»
(профиль «Безопасность автоматизированных систем»).**

Общая трудоемкость дисциплины составляет 3 зачетные единицы.

Форма контроля: зачёт.

Предполагаемые семестры: 5.

Целью изучения дисциплины является подготовка выпускников к деятельности, связанной с разработкой, внедрением и эксплуатацией инженерно-технических методов и средств защиты информации в автоматизированных системах управления и обработки информации.

Задачами курса являются:

- изучение технических каналов утечки информации и возможностей технических разведок;
- изучение способов и средств защиты информации от утечки по техническим каналам;
- освоение методов и средств контроля эффективности технической защиты информации.

Учебная дисциплина «Техническая защита информации» входит в профессиональный цикл (вариативная часть) и относится к числу специальных дисциплин и определяет теоретические основы и практические навыки, при освоении которых студент способен приступить к изучению следующих дисциплин в соответствии с учебным планом:

- Программно-аппаратные средства защиты информации;
- Технология построения защищённых автоматизированных систем;

- Методы выявления нарушений информационной безопасности;
- Комплексное обеспечение информационной безопасности автоматизированных систем;
- Противодействие техническим разведкам.

Краткое содержание дисциплины:

Теоретические основы инженерно-технической защиты информации.

Физические основы инженерно-технической защиты информации.

Технические средства добывания и защиты информации.

Методическое обеспечение инженерно-технической защиты информации.

В результате изучения дисциплины бакалавр должен обладать следующими общекультурными компетенциями (ОК):

ОК-7: способностью осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности, готовностью и способностью к активной созидательной деятельности в условиях информационного противоборства.

профессиональными компетенциями:

ПК-1: способностью использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности;

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 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;

эксплуатационная деятельность:

ПК-9: способностью принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия;

ПК-11: способностью выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации;

проектно-технологическая деятельность:

ПК-12: способностью участвовать в разработке подсистем управления информационной безопасностью;

ПК-13: способностью к проведению предварительного технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности;

ПК-18: способностью собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности;

экспериментально-исследовательская деятельность:

ПК-19: способностью составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности;

ПК-21: способностью проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов;

ПК-23: способностью принимать участие в проведении экспериментально-исследовательских работ системы защиты информации с учётом требований по обеспечению информационной безопасности;

ПК-24: способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности;

организационно-управленческая деятельность:

ПК-27: способностью принимать участие в организации контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации;

ПК-28: способностью изучать и обобщать опыт работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации;

ПК-30: способностью применять комплексный подход к обеспечению информационной безопасности в различных сферах деятельности.

**Аннотация к рабочей программе
дисциплины «Технологии и методы программирования»
по направлению 090900.62 Информационная безопасность
профиль Безопасность АС**

Общая трудоемкость дисциплины составляет 180 часов 5 зачетных единиц

Форма контроля: экзамен

Предполагаемые семестры: 3

Целью изучения дисциплины (модуля) является подготовка выпускников к деятельности, связанной с разработкой программного обеспечения для решения профессиональных задач.

Задачами курса является: развитие у слушателей логического мышления, способности математической формализации прикладных задач, создания алгоритмов и их анализа, овладения навыками программной реализации алгоритмов.

Учебная дисциплина относится к циклу БЗ. Для освоения дисциплины необходимы знания, полученные при изучении следующих дисциплин:

- информатика;
- языки программирования;
- иностранный язык (английский).

В дисциплине «Технологии и методы программирования» определяются теоретические основы и практические навыки, при освоении которых студент способен приступить к изучению следующих дисциплин в соответствии с учебным планом:

- программно-аппаратные средства защиты информации;
- криптографические методы защиты информации.

Знания и практические навыки, полученные в результате освоения дисциплины «Технологии и методы программирования», используются студентами при разработке курсовых и дипломных работ, в научно-исследовательской работе.

Краткое содержание дисциплины

Структуры данных

Алгоритмы сортировки

Алгоритмы поиска

Алгоритмы на графах

Генерация псевдослучайных последовательностей и алгоритмы порождения перестановок

В результате изучения дисциплины выпускник должен обладать следующими профессиональными компетенциями (ПК):

ПК-15: способностью применять программные средства системного, прикладного и специального назначения;

ПК-16: способностью разрабатывать научно техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ;

ПК-17: способностью применять методы анализа прикладной области на концептуальном, логическом, математическом и алгоритмическом уровнях.

Аннотация к рабочей программе дисциплины «Технология построения защищенных автоматизированных систем»

**по направлению 090900.62 Информационная безопасность
профиль подготовки «Безопасность автоматизированных систем»)**

Общая трудоемкость дисциплины составляет 4 зачетные единицы

Форма контроля: экзамен

Предполагаемые семестры: 7

Целью изучения дисциплины «Технология построения защищенных автоматизированных систем» является приобретение теоретических знаний и навыков работы, необходимых для разработки и эксплуатации автоматизированных систем,

информационные ресурсы которых содержат конфиденциальную информацию.

Задачи курса является изучить:

- принципы построения информационных систем;
- принципы организации информационных систем в соответствии с требованиями по защите информации;
- основные нормативные правовые акты в области информационной безопасности и защиты, а также нормативные методические документы ФСБ РФ;
- меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты;
- угрозы информационной безопасности объекта;
- отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем;
- методы и средства выявления угроз безопасности АС; методы технической защиты информации.

Приобрести навыки организации и обеспечения режима секретности.

Учебная дисциплина «Технология построения защищенных автоматизированных систем» является самостоятельным элементом в системе подготовки специалиста, относится к циклу БЗ.В4. Для освоения дисциплины необходимы знания, полученные при изучении следующих дисциплин:

- основы информационной безопасности;
- принципы построения, проектирования и эксплуатации автоматизированных информационных систем;
- информационная безопасность открытых систем.

В дисциплине «Технология построения защищенных автоматизированных систем» определяются теоретические основы и практические навыки, при освоении которых студент способен приступить к изучению следующих дисциплин в соответствии с учебным планом:

- комплексное обеспечение информационной безопасности АС;
- интегрированные информационные системы в управлении.

Краткое содержание дисциплины

Нормативно-методическая база создания защищенных автоматизированных систем (ЗАС). Классификация защищенных автоматизированных систем (ЗАС). Функциональные требования к компонентам ЗАС. Стадии и этапы создания ЗАС и требования по защите информации. Синтез программно-аппаратных средств ЗАС. Надежность и отказоустойчивость. Технологическая безопасность. Методы оценки защищенности автоматизированной системы. Мониторинг и защита от вторжений. Аудит безопасности ЗАС и управление рисками. Управление безопасностью ЗАС.

В результате изучения дисциплины специалист должен обладать следующими профессиональными компетенциями:

ОК-8: способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления;

ОК-9: способностью логически верно, аргументировано и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии.

ОК-11: способностью к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства.

ПК-5: способностью организовывать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом 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;

ПК-7: способностью использовать основные методы защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий.

ПК-8: способностью 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

ПК-25: способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных требований по защите информации;

ПК-26: способностью проводить инструментальный мониторинг защищенности автоматизированных систем.

**Аннотация к рабочей программе
дисциплины «Физическая культура»
по направлению 090900.62 Информационная безопасность
(профиль «Безопасность автоматизированных систем»)**

Общая трудоемкость дисциплины составляет 2 зачетных единиц.

Форма контроля: зачёт.

Предполагаемые семестры: 1,2,3,4

Целями освоения учебной дисциплины являются: формирование физической культуры личности и способности направленного использования разнообразных средств физической культуры, спорта и туризма для укрепления и сохранения здоровья, психофизической подготовки и самоподготовки к будущей профессиональной деятельности.

Задачами курса являются: формирование понимания социальной роли физической культуры в развитии личности и подготовка её к профессиональной деятельности; знание научно-биологических и практических основ физической культуры и здорового образа жизни; формирование мотивационно-целостного отношения к физической культуре, установки на здоровый образ жизни, человеческое самосовершенствование и самовоспитание потребности к регулярным занятиям физическими упражнениями и спортом; овладение системой практических умений и навыков, обеспечивающих сохранение и укрепление здоровья, психическое благополучие, развитие и совершенствование психофизических способностей, качеств и свойств личности, самоопределение в физической культуре; обеспечение общей и профессионально-прикладной физической подготовленности; определяющей готовность студента к будущей профессии; приобретение опыта творческого использования физкультурно-

спортивной деятельности для достижения жизненных и профессиональных целей; свести к минимуму травматизм при физической активности молодых людей – студентов высших учебных заведений.

Учебная дисциплина «Физическая культура» относится к циклу Б4.Б1

Краткое содержание дисциплины:

- основы здорового образа жизни;
- теория и методика физической культуры;
- основы техники: бега на короткие и длинные дистанции, прыжков, лыжных ходов, спортивных игр (волейбол, баскетбол, настольный теннис);
- содержание и методика профессионально-прикладной физической культуры;
- методические основы построения самостоятельных занятий по физическому воспитанию;
- методика самоконтроля на занятиях физической культуры.

В результате изучения дисциплины бакалавр должен обладать следующими общекультурными компетенциями:

ОК-12 способностью критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков;

ОК-13 способностью к самостоятельному применению методов физического воспитания для повышения адаптационных резервов организма и укрепления здоровья, готовностью к достижению должного уровня физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности.

Аннотация к рабочей программе дисциплины «Экономика» по направлению 090900.62 Информационная безопасность (Профиль «Безопасность автоматизированных систем»).

Общая трудоемкость дисциплины составляет 3 зачетных единиц.

Форма контроля: зачет.

Предполагаемые семестры: 6.

Цель освоения учебной дисциплины – дать студентам необходимые знания в области экономических отношений, опосредующих профессиональную деятельность бакалавров.

Задачами курса являются:

- изучить теоретические основы и закономерности функционирования экономики, включая трансформационные процессы;
- получить представления о принципах принятия и реализации экономических и управленческих решений;
- изучить подходы современных экономических школ и теории национальной экономики;
- рассмотреть основы современной государственной экономической политики.

«Экономика» как учебная дисциплина в системе подготовки специалиста связана с дисциплинами учебного плана «Философия», «История» и создают основу для изучения профессиональных компетенций.

Указанные связи дисциплины «Экономика» дают студенту системное представление о взаимосвязанности процессов материально-технических и социально-экономических, что призвано обеспечить соответствующий уровень и практическую

направленность в системе обучения деятельности специалистов.

Краткое содержание дисциплины:

Введение в экономическую теорию.

Основные понятия экономической науки.

Основные элементы хозяйствования, независимые от экономической системы.

Основы рыночной экономики.

Механизм индивидуальных рынков: спрос, предложение, цена.

Рынок и государство в современной экономике.

Механизм функционирования частного сектора.

Теория ценовой эластичности спроса. Эластичность предложения.

Государственные цены.

Теория потребительского поведения.

Теория издержек производства.

Теория чистой совершенной конкуренции. Максимизация прибыли.

Теории несовершенной конкуренции.

Теории заработной платы, человеческого капитала, экономической прибыли.

Теории ссудного капитала, земельной ренты.

Макроэкономика как объект анализа.

Теория определения уровня дохода. Теория мультипликатора.

Модели макроэкономической динамики.

Теории цикла. Принцип акселерации.

Теории занятости. Безработица. Закон Оукена.

В результате изучения дисциплины бакалавр должен обладать следующими профессиональными компетенциями:

- способностью формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности (ПК-4);

- способностью к проведению предварительного технико-экономического анализа обоснования проектных решений по обеспечению информационной безопасности (ПК-13).

**Аннотация к рабочей программе
дисциплины «Электротехника и схемотехника»
по направлению 090900 «Информационная безопасность»
(профиль подготовки «Безопасность автоматизированных систем»)**

Общая трудоемкость дисциплины: составляет 3 зачетные единицы.

Форма контроля: зачет.

Преподаваемые семестры: 4.

Целями освоения учебной дисциплины являются: формирование понимания у студентов принципов работы электронных и электротехнических устройств входящих в состав современной радиоэлектронной аппаратуры. О принципах проектирования и исследования схем электронных устройств радиотехники и связи, вычислительной

техники, автоматики.

Задачами курса являются:

- освоение основных понятий и терминов в области электроники;
- формирование у студентов понимания принципов работы электронных и электротехнических устройств, входящих в состав современной радиоэлектронной аппаратуры автоматизированных систем управления и вычислительных комплексов;
- формирование у студентов представления о принципах проектирования и исследования схем электронных устройств радиотехники и связи, вычислительной техники, автоматики;
- изучение типовых электронных схем и блоков.
- получение практических навыков расчета электрических и электронных схем..

Дисциплина относится к базовой части естественнонаучного цикла, в которой студенты изучают теоретические основы и получают практические навыки для изучения учебных дисциплин естественнонаучного и профессионального цикла.

Знания, полученные по дисциплине «Электротехника и схемотехника», непосредственно используются при изучении дисциплин базового цикла:

- аппаратные средства вычислительной техники;
- программно-аппаратные средства защиты информации;
- техническая защита информации;
- противодействие техническим разведкам;
- моделирование информационной безопасности автоматизированных систем;
- техническая защита информации.

Краткое содержание дисциплины:

1. Полупроводниковые элементы устройств радиотехники и автоматики.
2. Вторичные источники питания.
3. Электронные источники и усилители и электрических сигналов.
4. Схемотехника цифровых устройств.

В результате изучения дисциплины бакалавр должен обладать следующими профессиональными компетенциями:

ПК-1: способность использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности;

ПК-9: способность принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия;

ПК-11: способность выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации;

ПК-14: способностью оформить рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности;

ПК-22: способность проводить эксперименты по заданной методике, обработку результатов, оценку погрешности и достоверности их результатов

ПК-27: способностью принимать участие в организации контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации.

**Аннотация к рабочей программе
дисциплины «Электротехника»
по направлению 090900 «Информационная безопасность»
(профиль подготовки «Безопасность автоматизированных систем»)**

Общая трудоемкость дисциплины составляет 3 зачетные единицы.

Форма контроля: зачет.

Преподаваемые семестры 3.

Целями освоения учебной дисциплины являются: является изучение электрических явлений, основных моментов при производстве, передаче, распределении и использовании электрической энергии, формирование понимания у студентов принципов работы и электротехнических устройств и методов анализа электрических цепей.

Задачами курса являются:

освоение основных понятий и терминов в области электротехники;

- формирование у студентов минимально необходимых знаний основных электротехнических законов и методов анализа электрических цепей;
- изучение электрических явлений, основных моментов при производстве, передаче, распределении и использовании электрической энергии, формировании сигналов связи;
- формирование у студентов понимания принципов работы электротехнических устройств;
- получение практических навыков расчета электрических схем.

Дисциплина относится к базовой части естественнонаучного цикла, в которой студенты изучают теоретические основы и получают практические навыки для изучения учебных дисциплин естественнонаучного и профессионального цикла.

Знания, полученные по дисциплине «Электротехника», непосредственно используются при изучении дисциплин базового цикла:

- электроника и схемотехника;
- аппаратные средства вычислительной техники;
- программно-аппаратные средства защиты информации;
- техническая защита информации;
- противодействие техническим разведкам;
- моделирование информационной безопасности автоматизированных систем;
- техническая защита информации.

Краткое содержание дисциплины:

5. Введение в курс электротехники и схемотехники.
6. Электрические цепи постоянного тока.
7. Электрические цепи переменного тока.
8. Электрические сигналы и методы их исследования.
9. Переходные процессы в линейных электрических цепях и методы их расчета.

В результате изучения дисциплины бакалавр должен обладать следующими профессиональными компетенциями:

ПК-1: способность использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности;

ПК-9: способность принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия;

ПК-11: способность выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации;

ПК-22: способность проводить эксперименты по заданной методике, обработку результатов, оценку погрешности и достоверности их результатов

ПК-27: способностью принимать участие в организации контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации.

**Аннотация к рабочей программе дисциплины
«Языки программирования»
по направлению 090900.62 «Информационная безопасность»
(профиль «Безопасность автоматизированных систем»)**

Общая трудоемкость дисциплины составляет 4 зачетных единиц.

Форма контроля: экзамен

Предполагаемые семестры: 1

Целью изучения дисциплины (модуля) является подготовка выпускников к деятельности, связанной с разработкой программного обеспечения для решения профессиональных задач.

Задачами курса являются:

- 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.

Учебная дисциплина относится к циклу БЗ. Для освоения дисциплины необходимы знания, полученные при изучении следующих дисциплин:

- математика;
- информатика;
- иностранный язык (английский).

В дисциплине «Языки программирования» определяются теоретические основы и практические навыки, при освоении которых студент способен приступить к изучению следующих дисциплин в соответствии с учебным планом:

- информатика 2 (Языки программирования);
- технологии и методы программирования;

- программно-аппаратные средства защиты информации»;
- криптографические методы защиты информации;
- безопасность систем баз данных;

Знания и практические навыки, полученные в результате освоения дисциплины «Языки программирования», используются студентами при разработке курсовых и дипломных работ, в научно-исследовательской работе.

Краткое содержание дисциплины:

Основные этапы решения задач. Общая характеристика языков программирования высокого уровня. Запись алгоритма с помощью блок-схем.

Работа в среде программирования Borland Delphi.

Основные элементы языка Object Pascal. Программы с линейной структурой.

Программы с разветвленной структурой.

Программы с циклической структурой.

Одномерные массивы. Сортировка массивов.

Поиск значений в массивах. Работа с файлами.

Строки. Записи. Подпрограммы.

Динамические структуры данных. Модули.

Объектно-ориентированный подход к программированию.

Организация списков в Object Pascal.

Работа с графикой и графическими примитивами.

В результате изучения дисциплины, специалист должен обладать следующими профессиональными компетенциями (ПК):

ПК-15: способностью применять программные средства системного, прикладного и специального назначения;

ПК-16: способностью использовать инструментальные средства и системы программирования для решения профессиональных задач;

ПК-17: способностью к программной реализации алгоритмов решения типовых задач обеспечения информационной безопасности.

Аннотация к рабочей программе

дисциплины «Физика»

по направлению 090900.62 Информационная безопасность

(профиль «Безопасность автоматизированных систем»).

Общая трудоемкость дисциплины составляет 8 зачетных единиц.

Форма контроля: экзамен, экзамен.

Семестры: 2, 3.

Целями освоения учебной дисциплины (модуля) являются формирование у студента знаний и навыков научного мировоззрения и современного физического мышления. Курс физики совместно с курсами физико-математического цикла составляет основу теоретической подготовки и играет роль фундаментальной физико-математической базы, без которой невозможна успешная деятельность бакалавра любого профиля.

Задачами курса являются: формирование целостного представления, умений и навыков: по теоретическим и практическим проблемам в изучении основных законов классической и современной физики, а также освоении методов физического исследования; формирование навыков самостоятельного, творческого использования теоретических и практических знаний при решении конкретных задач; формирование навыков работы с современной научной аппаратурой; формирование навыков проведения физического эксперимента; применение полученных навыков и умений в профессиональной деятельности.

Учебная дисциплина «Физика» входит в математический и естественнонаучный цикл (базовая часть) и относится к числу фундаментальных дисциплин, поскольку служит основой для изучения учебных дисциплин как математического и естественнонаучного, так и профессионального цикла.

Знания, полученные по дисциплине «Физика», непосредственно используются при изучении дисциплин базового цикла:

- «Математика»;
- «Информатика»;
- «Теория информации»;
- «Теория вероятностей и математическая статистика»;
- «Дискретная математика».

и дисциплин профессионального цикла:

- «Основы информационной безопасности»;
- «Аппаратные средства вычислительной техники»;
- «Программно-аппаратные средства защиты информации»;
- «Криптографические методы защиты информации»;
- «Техническая защита информации»;
- «Организационное и правовое обеспечение информационной безопасности»;
- «Сети и системы передачи информации»;
- «Безопасность жизнедеятельности»;
- «Языки программирования»;
- «Технология и методы программирования»;
- «Управление информационной безопасностью»;
- «Документоведение»;
- «Электротехника»;
- «Электротехника и схемотехника»;

Краткое содержание дисциплины:

Физические основы механики. Элементы кинематики. Динамика частиц. Система материальных точек. Законы сохранения энергии, импульса, момента импульса. Элементы механики сплошных сред

Основы молекулярно-кинетической теории. Микроскопическое состояние вещества. Статистические распределения. Основы термодинамики. Явления переноса.

Электростатика. Постоянный электрический ток. Электрический ток в металлах и вакууме.

Магнитное поле. Электромагнитная индукция. Магнитные свойства вещества.

Основы теории Максвелла.

Механические и электромагнитные колебания. Электромагнитные волны.

Элементы геометрической и электронной оптики. Элементы фотометрии. Волновая оптика.

Квантовая природа излучения. Экспериментальное обоснование идей квантовой теории. Квантовое состояние. Уравнение Шредингера.

Атом. Модели атома. Атомное ядро.

Основы физики твердого тела.

Элементы физики элементарных частиц.

Современная физическая картина мира.

В результате изучения дисциплины бакалавр должен обладать следующими общекультурными и профессиональными компетенциями:

ОК-9: способностью логически верно, аргументированно и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии;

ОК-12: способностью критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков;

ПК-1: способностью использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности;

ПК-2: способностью 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;

ПК-18: способностью собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности;

ПК-19: способностью составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности;

ПК-20: способностью применять методы анализа изучаемых явлений, процессов и проектных решений;

ПК-22: способностью проводить эксперименты по заданной методике, обработку результатов, оценку погрешности и достоверности их результатов;

ПК-23: способностью принимать участие в проведении экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности;

ПК-24: способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности;

