МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФГБОУ ВПО «Дагестанский государственный технический университет»

УТВЕРЖДАЮ:
Ректор
Председатель Ученого совета
Исмаилов Т.А.
«22» апреля 2011г.

Рекомендовано к утверждению
Проректор по УР
Председатель методического совета
Гасанов К.А.
«22» апреля 2011г.

Номер внутривузовской регистрации

ОСНОВНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

Специальность
090303.65 - Информационная безопасность автоматизированных систем

Специализация
Безопасность открытых информационных систем

Квалификация (степень)

Специалист

Форма обучения
очная

Декан факультета _____ Мустафаев А.Г.
Зав. кафедрой _____ Ильясов Э.Э.

Махачкала 2011

Согласовано:

Проректор по НРиИ _____ Юсуфов Ш.А.

Проректор по ВРиГО _____ Ю.Н. Абдулкадыров

Начальник УО _____ Атаханов Р.А.

Начальник ОМО _____ Меджидова Л.М.

Оглавление

1. Общие положения

1.1. Определение основной образовательной программы

Основная образовательная программа специальности 090303.65 - Информационная безопасность автоматизированных систем представляет собой систему документов, разработанную выпускающей кафедрой, согласованную в установленном порядке и утвержденную ректором университета с учетом требований рынка труда на основе Федерального государственного образовательного стандарта по соответствующему направлению подготовки высшего профессионального образования (ФГОС ВПО), а также с учетом рекомендованной примерной основной образовательной программы.

ООП регламентирует цели, ожидаемые результаты, содержание, условия и технологии реализации образовательного процесса, оценку качества подготовки выпускника по данному направлению подготовки и включает в себя.

1.2. Нормативные документы для разработки ООП специальности 090303.65 - Информационная безопасность автоматизированных систем

Нормативную правовую базу разработки ООП специальности составляют:

- Федеральные законы Российской Федерации: «Об образовании» и «О высшем и послевузовском профессиональном образовании»;
- типовое положение об образовательном учреждении высшего профессионального образования (высшем учебном заведении), утвержденное постановлением Правительства Российской Федерации;
- Федеральный государственный образовательный стандарт по специальности 090303.65 Информационная безопасность автоматизированных систем высшего профессионального образования, утвержденный приказом Министерства образования и науки Российской Федерации от «17» января 2011г. № 60 (Приложение 1);
- дополнение к ФГОС ВПО по специальности 090303.65- Информационная безопасность автоматизированных систем с дисциплинами вариативной части с учетом профиля подготовки и с представлением учебных

циклов, разделов, трудоемкости, в зачетных единицах и в часах, перечня дисциплин для разработки программ (Приложение 2);

- примерная ООП ВПО с примерным учебным планом, рекомендованные учебно-методическим объединением по направлению (специальности) (Приложение 3);
- нормативно-методические документы Минобрнауки России;
- устав ФГБОУ ВПО «Дагестанский государственный технический университет»;
- внутривузовская система управления качеством подготовки специалистов.

1.3. Общая характеристика основной образовательной программы высшего профессионального образования

1.3.1. Цель ООП по специальности 090303.65 - Информационная безопасность автоматизированных систем

ООП специальности 090303.65 - Информационная безопасность автоматизированных систем имеет своей целью развитие у студентов таких личностных качеств, как ответственность, толерантность, стремление к саморазвитию и раскрытию своего творческого потенциала, владение культурой мышления, стремление к воплощению в жизнь гуманистических идеалов, осознание социальной значимости профессии связанной с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере, способность принимать организационные решения в стандартных ситуациях и готовность нести за них ответственность, умение критически оценивать собственные достоинства и недостатки, выбирать пути и средства развития первых и устранения последних, формирование общекультурных универсальных (общенаучных, социально-личностных, инструментальных) компетенций.

Целью ООП по специальности 090303.65 - Информационная безопасность

автоматизированных систем является также формирование профессиональных компетенций, таких как понимание сущности и социальной значимости профессии, основных перспектив и проблем, определяющих конкретную область деятельности; владение основами теории фундаментальных разделов математики (математического анализа, алгебры, геометрии, теории вероятностей и математической статистики); физики, владение навыками, охватывающими совокупность проблем направленными на обеспечение защищенности объектов информатизации в условиях существования угроз в информационной сфере.

Специалист по защите информации в условиях развития науки и техники должен быть готов к критической оценке накопленного опыта и творческому анализу своих возможностей, способен использовать навыки работы с информацией от различных источников для решения профессиональных и социальных задач; понимать основные возможности приобретения новых знаний с использованием современных научных методов и владение ими на уровне, необходимом для решения задач, имеющих естественнонаучное содержание и возникающих при выполнении профессиональных функций.

1.3.2. Срок освоения ООП специальности

В соответствии с разделом III ФГОС срок освоения ООП специальности, включая каникулы, предоставляемые после прохождения итоговой государственной аттестации, составляет 5 (пять) лет при очной форме обучения.

1.3.3. Трудоемкость ООП специальности

В соответствии с разделом III ФГОС общая трудоемкость программы специальности, включая теоретическое обучение, сессии, практики, итоговую государственную аттестацию и каникулы, составляет 300 зачетных единиц (260 недель).

1.4. Требования к абитуриенту

Абитуриент должен иметь документ государственного образца о среднем (полном) общем образовании или среднем профессиональном образовании.

2. Характеристика профессиональной деятельности выпускника ООП

по специальности 090303.65 - Информационная безопасность автоматизированных систем

2.1. Область профессиональной деятельности выпускника

В соответствии с п. 4.1 ФГОС область профессиональной деятельности специалистов включает: сферы науки, техники и технологии, охватывающие совокупность проблем, связанных с обеспечением информационной безопасности автоматизированных систем в условиях существования угроз в информационной сфере.

2.2. Объекты профессиональной деятельности выпускника

В соответствии с п. 4.2 ФГОС объектами профессиональной деятельности специалистов являются: автоматизированные системы, функционирующие в условиях существования угроз в информационной сфере и обладающие информационно-технологическими ресурсами, подлежащими защите; информационные технологии, формирующие информационную инфраструктуру в условиях существования угроз в информационной сфере и задействующие информационно-технологические ресурсы, подлежащие защите; технологии обеспечения информационной безопасности автоматизированных систем; системы управления информационной безопасностью автоматизированных систем.

2.3. Виды профессиональной деятельности выпускника специальности 090303.65 - Информационная безопасность автоматизированных систем готовится к следующим видам профессиональной деятельности:

научно-исследовательская;

проектно-конструкторская;

контрольно-аналитическая;

организационно-управленческая;

эксплуатационная.

Конкретные виды профессиональной деятельности, к которым в основном готовится специалист, определяются высшим учебным заведением совместно с

обучающимися, научно-педагогическими работниками высшего учебного заведения и объединениями работодателей.

По окончании обучения по направлению подготовки (специальности) **090303 Информационная безопасность автоматизированных систем,** наряду с квалификацией (степенью) «специалист» присваивается специальное звание «специалист по защите информации».

2.4. Задачи профессиональной деятельности выпускника

В соответствии с п. 4.4 ФГОС специалист по специальности **090303.65 - Информационная безопасность автоматизированных систем** должен решать следующие профессиональные задачи в соответствии с видами профессиональной деятельности:

научно-исследовательская деятельность:

сбор, обработка, анализ и систематизация научно-технической информации, отечественного и зарубежного опыта по проблемам информационной безопасности автоматизированных систем;

подготовка научно-технических отчетов, обзоров, публикаций по результатам выполненных исследований;

моделирование и исследование защищенных автоматизированных систем, анализ их уязвимостей и эффективности средств и способов защиты;

анализ безопасности информационных технологий, реализуемых в автоматизированных системах;

разработка эффективных решений по обеспечению информационной безопасности автоматизированных систем;

проектно-конструкторская деятельность:

сбор и анализ исходных данных для проектирования систем защиты информации;

разработка политик информационной безопасности автоматизированных систем;

разработка защищенных автоматизированных систем по профилю профес-

сиональной деятельности, обоснование выбора способов и средств защиты информационно-технологических ресурсов автоматизированных систем;

выполнение проектов по созданию программ, комплексов программ, программно-аппаратных средств, баз данных, компьютерных сетей для защищенных автоматизированных систем;

разработка системы управления информационной безопасностью автоматизированных систем;

контрольно-аналитическая:

контроль работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации;

экспериментально-исследовательские работы при сертификации средств защиты автоматизированных систем;

экспериментально-исследовательские работы при аттестации автоматизированных систем;

инструментальный мониторинг защищенности автоматизированных систем;

организационно-управленческая деятельность:

организация работы коллектива, принятие управленческих решений в условиях спектра мнений, определение порядка выполнения работ;

разработка предложений по совершенствованию и повышению эффективности принятых мер по обеспечению информационной безопасности автоматизированных систем;

организация работ по выполнению требований защиты информации ограниченного доступа;

методическое и организационное обеспечение информационной безопасности автоматизированных систем;

организация работ по созданию, внедрению, эксплуатации и сопровождению защищенных автоматизированных систем;

контроль реализации политики информационной безопасности;

эксплуатационная деятельность:

реализация информационных технологий в сфере профессиональной деятельности с использованием защищенных автоматизированных систем;

администрирование подсистем информационной безопасности автоматизированных систем;

мониторинг информационной безопасности автоматизированных систем;

управление информационной безопасностью автоматизированных систем;

обеспечение восстановления работоспособности систем защиты информации при возникновении нештатных ситуаций.

3. Компетенции выпускника ООП специальности, формируемые в результате освоения данной ООП ВПО

Результаты освоения ООП специальности определяются приобретаемыми выпускником компетенциями, т.е. его способностью применять знания, умения и личные качества в соответствии с задачами профессиональной деятельности.

3.1. Выпускник должен обладать следующими общекультурными компетенциями (ОК):

способностью действовать в соответствии с Конституцией Российской Федерации, исполнять свой гражданский и профессиональный долг, руководствуясь принципами законности и патриотизма (ОК-1);

способностью осуществлять свою деятельность в различных сферах общественной жизни с учетом принятых в обществе морально-нравственных и правовых норм, соблюдать принципы профессиональной этики (ОК-2);

способностью анализировать социально значимые явления и процессы, в том числе политического и экономического характера, мировоззренческие и философские проблемы, применять основные положения и методы гуманитарных, социальных и экономических наук при решении социальных и профессиональных задач (ОК-3);

способностью понимать движущие силы и закономерности исторического процесса, роль личности в истории, политической организации общества, спо-

собностью уважительно и бережно относиться к историческому наследию, толерантно воспринимать социальные и культурные различия (ОК-4);

способностью понимать социальную значимость своей будущей профессии, цели и смысл государственной службы, обладать высокой мотивацией к профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства (ОК-5);

способностью к работе в коллективе, кооперации с коллегами, способностью в качестве руководителя подразделения, лидера группы сотрудников формировать цели команды, принимать организационно-управленческие решения в нестандартных ситуациях и нести за них ответственность, предупреждать и конструктивно разрешать конфликтные ситуации в процессе профессиональной деятельности (ОК-6);

способностью логически верно, аргументировано и ясно строить устную и письменную речь на русском языке, готовить и редактировать тексты профессионального назначения, публично представлять собственные и известные научные результаты, вести дискуссии (ОК-7);

способностью к письменной и устной деловой коммуникации, к чтению и переводу текстов по профессиональной тематике на одном из иностранных языков (ОК-8);

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

способностью самостоятельно применять методы и средства познания, обучения и самоконтроля для приобретения новых знаний и умений, в том числе в новых областях, непосредственно не связанных со сферой профессиональной деятельности, развития социальных и профессиональных компетенций, к изменению вида своей профессиональной деятельности (ОК-10);

способностью к воспитательной и образовательной деятельности (ОК-11);

способностью самостоятельно применять методы физического воспитания для повышения адаптационных резервов организма и укрепления здоровья, достижения должного уровня физической подготовленности в целях обеспечения полноценной социальной и профессиональной деятельности (ОК-12).

3.2. Выпускник должен обладать следующими профессиональными компетенциями (ПК):

общепрофессиональными:

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

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

способностью использовать языки, системы и инструментальные средства программирования в профессиональной деятельности (ПК-3);

способностью понимать сущность и значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска и обработки больших объемов информации по профилю деятельности в глобальных компьютерных системах, сетях, в библиотечных фондах и в иных источниках информации (ПК-4);

способностью применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ПК-5);

способностью использовать нормативные правовые акты в своей профессиональной деятельности (ПК- 6);

способностью использовать основные методы защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных

бедствий (ПК- 7);

способностью к освоению новых образцов программных, технических средств и информационных технологий (ПК-8);

в научно - исследовательской деятельности:

способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере своей профессиональной деятельности (ПК-9);

способностью применять современные методы исследования с использованием компьютерных технологий (ПК-10);

способностью разрабатывать и исследовать модели автоматизированных систем (ПК-11);

способностью проводить анализ защищенности автоматизированных систем (ПК-12);

способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы (ПК-13);

способностью проводить анализ рисков информационной безопасности автоматизированной системы (ПК-14);

способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем (ПК-15);

способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ (ПК-16);

• в проектно-конструкторской деятельности:

способностью проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем (ПК-17);

способностью участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности (ПК-18);

способностью участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности (ПК-19);

способностью разрабатывать политики информационной безопасности автоматизированных систем (ПК-20);

способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы (ПК-21);

способностью участвовать в проектировании средств защиты информации и средств контроля защищенности автоматизированной системы (ПК-22);

в контрольно-аналитической деятельности:

• способностью проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-23);

• способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты автоматизированных систем (ПК-24);

• способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных требований по защите информации (ПК-25);

• способностью проводить инструментальный мониторинг защищенности автоматизированных систем (ПК-26);

• в организационно-управленческой деятельности:

способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности (ПК-27);

способностью разрабатывать оперативные планы работы первичных подразделений (ПК-28);

способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы (ПК-29);

способностью организовать эксплуатацию автоматизированной системы с учетом требований информационной безопасности (ПК-30);

способностью разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, а также положений, инструкций и других организационно-распорядительных документов в сфере профессиональной деятельности (ПК-31);

способностью проводить анализ особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите (ПК-32);

способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации (ПК-33);

• способностью формировать комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной системы (ПК-34);

• в эксплуатационной деятельности:

способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности (ПК-35);

способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы (ПК-36);

способностью администрировать подсистему информационной безопасности автоматизированной системы (ПК-37);

способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы (ПК-38);

способностью управлять информационной безопасностью автоматизированной системы (ПК-39);

способностью обеспечить восстановление работоспособности систем защиты информации при возникновении нештатных ситуаций (ПК-40).

Специализация № 4 «Безопасность открытых информационных систем»:

способностью проводить анализ и исследовать модели защищенности открытых информационных систем (ПСК-4.1);

способностью участвовать в разработке компонентов открытых информационных систем (ПСК-4.2);

способностью обеспечить эффективное применение информационно-технологических ресурсов открытых информационных систем с учетом нормативных требований по защите информации (ПСК-4.3);

способностью разрабатывать и реализовывать политики информационной безопасности открытых информационных систем (ПСК-4.4);

способностью участвовать в проектировании и эксплуатации системы управления информационной безопасностью открытой информационной системы (ПСК-4.5);

• способностью проводить инструментальный мониторинг защищенности открытых информационных систем (ПСК-4.6);

способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью открытой информационной системы (ПСК-4.7);

• способностью формировать и эффективно применять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности открытых информационных систем (ПСК-4.8).

4. Документы, регламентирующие содержание и организацию образовательного процесса при реализации ООП по специальности 090303.65 - Информационная безопасность автоматизированных систем

В соответствии с Типовым положением о вузе, Уставом университета и ФГОС ВПО специальности содержание и организация образовательного процесса при реализации данной ООП регламентируется учебным планом; рабочими программами учебных курсов, предметов, дисциплин (модулей); материалами, обеспечивающими качество подготовки и воспитания

обучающихся; программами учебных и производственных практик; годовым календарным графиком учебного процесса, а также методическими материалами, обеспечивающими реализацию соответствующих образовательных технологий.

4.1. График учебного процесса и учебный план

График учебного процесса отражает последовательность реализации ООП ВПО по годам, включая теоретическое обучение, практики, промежуточные и итоговую аттестации, каникулы, и входит в структуру учебного плана.

Учебный план подготовки специалиста по Информационной безопасности автоматизированных систем составлен по циклам учебных дисциплин и разделам, содержит базовую и вариативную части, включает перечень дисциплин, их трудоемкость и примерную последовательность изучения. Базовая часть, представленная в учебных циклах С.1-С.3, и содержание раздела С.4 согласно ФГОС подготовки специалистов по Информационной безопасности автоматизированных систем являются общими, т.е. независящими от специализации.

Дисциплины по выбору циклов С.1-С.3 сформированы с учетом реализуемой в ДГТУ специализации – «Безопасность открытых информационных систем».

График учебного процесса и учебный план приведены в Приложении 4.

4.2. Рабочие программы дисциплин учебного плана

Рабочие программы по всем дисциплинам разработаны и находятся на кафедре. Аннотации к рабочим программам дисциплин приведены в Приложении 5.

4.3. Программы практик

Программы учебной, производственной и преддипломной практик приведены в Приложении 6.

5. Фактическое ресурсное обеспечение ООП по специальности 090303.65 - Информационная безопасность автоматизированных систем

Фактическое ресурсное обеспечение данной ООП формируется на основе требований к условиям реализации ООП специалитета, определяемых ФГОС ВПО по специальности 090303.65 - Информационная безопасность автоматизированных систем, с учетом рекомендаций соответствующей ПрООП, и включает в себя кадровое, учебно-методическое, информационное и материально-техническое обеспечения учебного процесса.

5.1. Кадровое обеспечение реализации ООП ВПО

Реализация основной образовательной программы по специальности 090303.65 -Информационная безопасность автоматизированных систем обеспечивается квалифицированными педагогическими кадрами.

Доля преподавателей, имеющих учёную степень и (или) учёное звание, в общем числе преподавателей, обеспечивающих образовательный процесс по данной основной образовательной программе, составляет 64% (в соответствии с п.7.16 ФГОС ВПО не менее 60%), учёную степень доктора наук и (или) учёное звание профессора имеют 39 % преподавателей (в соответствии с ФГОС ВПО не менее 8% преподавателей).

Преподаватели профессионального цикла имеют базовое образование и (или) учёную степень, соответствующие профилю дисциплины. 69% преподавателей, обеспечивающих учебный процесс по профессиональному циклу, имеют учёные степени (в соответствии с ФГОС ВПО не менее 60% преподавателей).

5.2. Учебно-методическое и информационное обеспечение учебного

процесса

Освоение данной ООП полностью обеспечено учебниками и учебными пособиями по дисциплинам (модулям) всех циклов учебного плана и практик.

Каждый обучающийся по ООП обеспечен не менее чем одним учебным и одним учебно-методическим печатным и/или электронным изданием по каждой дисциплине профессионального цикла, входящей в образовательную программу (включая электронные базы периодических изданий).

Библиотечный фонд укомплектован печатными и/или электронными изданиями основной учебной литературы по дисциплинам базовой части всех циклов, изданными за последние 10 лет (для дисциплин базовой части гуманитарного, социального и экономического цикла – за последние 5 лет). Из имеющейся учебной литературы более 50 % наименований имеют гриф Минобрнауки России и профильных УМО. Доля новых поступлений по циклу ОПД составляет 70 % от общего книжного фонда по данному циклу дисциплин.

Фонд дополнительной литературы помимо учебной включает официальные справочно-библиографические и периодические издания в расчете 1-2 экземпляра на каждые 100 обучающихся.

Для студентов имеется доступ к комплектам библиотечного фонда отечественных и зарубежных академических и отраслевых журналов по специальности 090303.65 -Информационная безопасность автоматизированных систем.

5.3. Материально-техническое обеспечение учебного процесса

Факультет КТВТиЭ ДГТУ располагает материально-технической базой, обеспечивающей проведение всех видов подготовки, лабораторной, практической и научно-исследовательской работы обучающихся, которые предусмотрены учебным планом, и соответствующей действующим санитарным и противопожарным правилам и нормам.

Учебно-лабораторная база университета и факультета включает лекционные (поточные и групповые) аудитории; лаборатории общих

практикумов по физике, электротехнике, электронике, БЖД; компьютерные классы для проведения лабораторных работ по языкам программирования, системам управления базами данных, операционным системам, аппаратным средствам вычислительной техники; специализированные лаборатории по сетям и средствам передачи информации, программно-аппаратным методам защиты информации, комплексным методам защиты информации, для проведения научно-исследовательских работ и др.

Имеющаяся материальная база обеспечивает:

- Проведение лекций – аппаратурой для демонстрации иллюстративного материала;
- Выполнение лабораторных занятий по базовым дисциплинам – учебно-научное оборудование в соответствии с программой лабораторного практикума;
- Выполнение лабораторных занятий по профильным (специальным) дисциплинам – учебно-научным и научным оборудованием в соответствии с реализуемой научной тематикой лаборатории;
- Проведение практических занятий – компьютерами для выполнения вычислений, занятия по иностранному языку – лингафонным кабинетом.

При изучении специальных дисциплин ООП специальности и выполнении выпускной квалификационной работы обучающимся предоставляется возможность использования научного оборудования университета, а также возможность пользования электронными изданиями через Интернет в компьютерных классах, а также в зале Центра современных информационных технологий ДГТУ, оснащенном 168 компьютерами.

ООП по специальности 090303.65 - Информационная безопасность автоматизированных систем реализуется с широким привлечением современной вычислительной техники и средств телекоммуникаций. Специальное программное обеспечение установлено во всех компьютерных классах. При этом все компьютеры подключены к университетской сети, имеющей выход в Интернет.

6. Характеристика среды вуза, обеспечивающие развитие общекультурных (социально-личностных) компетенций выпускников

Воспитательная среда Дагестанского государственного технического университета в целом и факультета КТВТиЭ в частности складывается из мероприятий, которые ориентированы на:

• формирование личностных качеств, необходимых для эффективной профессиональной деятельности выпускника;

• воспитание нравственных качеств, интеллигентности, развитие ориентации на общечеловеческие ценности и высокие гуманистические идеалы культуры;

• привитие умений и навыков управления коллективом в различных формах студенческого самоуправления;

• сохранение и приумножение историко-культурных традиций университета, преемственности, формирование чувства университетской солидарности, формирование у студентов патриотического сознания;

• укрепление и совершенствование физического состояния, стремление к здоровому образу жизни, воспитание нетерпимого отношения к наркотикам, пьянству, антиобщественному поведению.

Воспитательная среда включает в себя три составляющей:

1. профессионально-трудовая,
2. гражданско-правовая,
3. культурно-нравственная.

6.1. Профессионально-трудовая составляющая воспитательной среды

специально организованный и контролируемый процесс приобщения студентов к профессиональному труду в ходе становления их в качестве субъектов этой деятельности, увязанный с овладением квалификацией и воспитанием профессиональной этики.

Задачи:

• подготовка профессионально-грамотного, компетентного,

ответственного сотрудника;

• формирование личностных качеств для эффективной профессиональной деятельности, таких как: трудолюбие, любовь к окружающей природе, рациональность, профессиональная этика, способность принимать ответственные решения, умение работать в коллективе, творческие способности и другие качества, необходимые выпускнику для будущей профессиональной деятельности;

• привитие умений и навыков управления коллективом.

Основные формы реализации:

• организация научно-исследовательской работы студентов;

• проведение ежегодных студенческих научных конференций, секция защиты информации;

• проведение университетских, областных (межвузовских) конкурсов на лучшие научно-исследовательские, квалификационные и курсовые работы;

• работа коллективов (кружков), опирающихся на научные исследования;

• мониторинг студенческой среды но вопросам организации учебного процесса;

• награждение студентов, достигших успехов как в науке, так и в общественной деятельности;

• проведение экскурсий в историко-краеведческий музей и музей изобразительных искусств.

6.2. Гражданско-правовая составляющая воспитательной среды - интеграция гражданского, правового, патриотического, интернационального, политического, семейного воспитания.

Задачи:

• формирование у студентов гражданской позиции и патриотического сознания, уважения к правам и свободам человека, любви к Родине, семье;

• формирование правовой и политической культуры;

• формирование установки на воспитание культуры семейных отношений, преемственность социокультурных традиций;

• формирование качеств, которые характеризуют связь личности и общества, гражданственность, патриотизм, толерантность, социальная активность, личная свобода, коллективизм, общественно-политическая активность и др.

Основные формы реализации:

• проведение Дня факультета;

• развитие студенческого самоуправления;

• организация субботников на факультете, в университете, в общежитиях для воспитания бережливости и чувства причастности к совершенствованию материально-технической базы университета;

• кураторство студенческих групп младших курсов, (куратор помогает на первом этапе знакомства студентов с университетской системой, организуя встречи во внеурочное время, походы в театр, на концерты, поездки на природу; поддерживает связь с родителями студентов-нарушителей и отстающих);

• совместное с преподавателями обсуждение проблем студенчества;

• дополнительное материальное стимулирование студентов, имеющих высокие показатели в учебе, НИРС, активистов;

• совместное со студентами проведение профориентационной работы в подшефных школах;

• социальная защита малообеспеченных категорий студентов;

• участие в программах государственной молодежной политики всех уровней.

6.3. Культурно-нравственная составляющая воспитательной среды включает в себя духовное, нравственное, эстетическое, экологические и физическое воспитание.

Задачи:

• воспитание нравственно развитой личности;

• воспитание эстетически и духовно развитой личности;

• формирование физически здоровой личности;

• формирование таких качеств личности, как высокая нравственность, эстетический вкус, положительные моральные, коллективистские, волевые и физические качества, нравственно-психологическая и физическая готовность к труду и служению Родине.

Основные формы реализации:

• развитие досуговой, клубной деятельности (КВН, День первокурсника, Студенческая весна и т.д.), поддержка молодежной субкультуры в рамках создания реального творческого процесса;

• организация выставок творчества студентов;

• участие в спортивных мероприятиях университета;

• проведение в общежитиях культурно-воспитательных мероприятий, помогающих студентам чувствовать себя психологически комфортно вдали от дома;

•анализ социально-психологических проблем студенчества и организация психологической поддержки;

•благотворительные мероприятия (например, сбор книг и игрушек, детских вещей для детей, организация концерта); организация встреч с интересными людьми (выпускниками, деятелями культуры др.) организация физического воспитания студентов,

•экологическое воспитание;

•организация санаторно-курортного лечения студентов с хроническими заболеваниями;

•социологические исследования жизнедеятельности студентов по различным направлениям, эффективности культурно-массовых и спортивных мероприятий, адаптации к вузу;

•профилактика наркомании, алкоголизма и других вредных привычек; борьба с курением; профилактики правонарушений;

•применение различных форм работы со студентами (тренинги, ролевые

игры и др.), проведение встреч с врачами, наркологами, эпидемиологами и другими специалистами;

•пропаганда здорового образа жизни, занятий спортом,

•работа студенческих самодеятельных коллективов, выступающих в университетских, городских и международных мероприятиях; работа творческих кружков.

7. Нормативно-методическое обеспечение системы оценки качества освоения обучающимися ООП специальности 090303.65 -Информационная безопасность автоматизированных систем

Нормативно-методическое обеспечение текущего контроля успеваемости и промежуточной аттестации обучающихся по ООП специальности осуществляется в соответствии с Типовым положением о вузе, Уставом ДГТУ, Положением о модульно-рейтинговой системе оценки учебной деятельности студентов:

Механизмом, обеспечивающим непрерывный контроль выполнения учебного плана, является модульно-рейтинговая система (МРС) оценки учебной деятельности, разработанная в соответствии с концепцией системы управления качеством подготовки специалистов в университете. Для реализации непрерывности контроля и осуществления обратной связи предусмотрены следующие формы контроля:

- текущий рейтинг студента по дисциплине (производится в течение семестра в период проведения текущих аттестаций (ТРд);
- рейтинг студента по текущим аттестациям (ТРа), определяемый по результатам текущих аттестаций как среднее арифметическое произведений набранных по каждой дисциплине баллов на весовые коэффициенты соответствующих дисциплин;
- рейтинг студента по дисциплине (семестровый дисциплинарный рейтинг) (СРд), рассчитываемый как суммарное количество баллов, набранных студентом при изучении дисциплины в течение всего семестра, т.е. сумма баллов

3х текущих аттестаций и баллов промежуточной аттестации (экзамена или зачета0 по этой дисциплине;

- рейтинг студента за семестр (семестровый рейтинг) (СР) или годовой (курсовой рейтинг) (КР), рассчитываемый как средневзвешенный рейтинг студента по всем семестровым дисциплинарным рейтингам за семестр с учетом весовых коэффициентов трудоемкости дисциплины;
- рейтинг студента за всю программу обучения (Рирг), определяемый как среднее значение соответствующих рейтингов студента за 1-й, 2-й, 3-й, 4-й и 5-й курсы обучения;
- итоговый рейтинг студента, складываемый из двух рейтинговых баллов, оцениваемых по 100-бальной шкале (ИР):

- рейтинговые баллы по итоговому междисциплинарному экзамену;

- рейтинговые баллы по защите ВКР.

- рейтинг студента выпускника – выпускной рейтинг (ВР), определяемый как среднее арифметическое рейтинга программы (Рирг) и рейтингов, полученных студентом на государственных экзаменах (междисциплинарный экзамен и защита выпускной квалификационной работы), т.е. итогового рейтинга (ИР).

Таким образом, из вышеизложенного следует, что модульно-рейтинговая система основана на интегральной оценке всех видов учебной (аудиторная, самостоятельная, практическая работа), а также научно-исследовательская деятельность студентов. Данная система позволяет усилить мотивацию их деятельности путем дифференциальной оценки результатов учебной работы каждого студента и снизить влияние субъективных факторов, что способствует повышению академической активность студента и качества подготовки специалиста.

Основными принципами формирования учебных модулей для модульно-рейтинговой системы оценки являются:

- повышение мотивации студентов к освоению основной образовательной программы (ООП) по направлению (специальности) путем

более высокой дифференциации оценки их учебной работы, для своевременной коррекции содержания и методики преподавания;

- *интенсификация самостоятельной работы студентов* за счет более рациональной организации обучения и постоянного контроля его результатов;
- *регулярность оценки* результатов работы студентов;
- *строгое соблюдение исполнительной дисциплины* всеми участниками образовательного процесса (студентами, профессорско-преподавательским составом, учебно-вспомогательным и административно-управленческим персоналам).

Цель текущего и промежуточного рейтинг-контроля – стимулировать в течение семестра регулярную работу студентов над изучаемым материалом, способствовать первичному усвоению знаний, обеспечивать функционирование оперативной обратной связи в процессе обучения.

Целями рубежного рейтинг-контроля (эквивалент зачета) и итогового рейтинг-контроля (эквивалент экзамена) являются:

а) предоставление студенту возможности сосредоточиться на осмыслении каждой конкретной дисциплины в целом с позиций системного подхода в специально выделенное для этого время по расписанию;

б) развитие навыков устного общения как в общекультурном плане, так и с использованием инженерного языка, учитывающего специфику предметной области;

в) предоставление преподавателю возможности интегрально оценить работу студента за весь курс (семестр).

Проведение внутрисеместрового контроля (текущего и промежуточного) является мощным и весьма эффективным стимулом ритмичной работы в течении всего семестра по всем видам занятий, предусмотренным учебным планом.

Результаты контроля в виде зачетов и экзаменов заносятся в ведомости.

В качестве балльной шкалы для рейтинговых оценок принята универсальная 100-балльная шкала. При подведении итогов обучения за семестр итоговый рейтинг переводится в оценку: в виде зачета (зачтено; не зачтено) или

дифференцированную (отлично, хорошо, удовлетворительно, неудовлетворительно).

Перевод рейтинговой оценки в зачетную осуществляется по правилу: не менее 56 баллов – зачтено, 55 баллов и менее – не зачтено.

Такой переход практически не требуется в период текущих аттестаций, так как по одной текущей аттестации может быть набрано по отдельной части ДМ, пройденной в период текущей аттестации, не более 28 баллов (20 баллов текущая аттестации, 5 баллов посещаемость и 3 бонусных балла из 5 бонусных семестровых баллов).

Порог успеваемости в рейтинговых баллах с учетом посещаемости должен:

- по итогам 1 аттестации – 15 баллов;
- по итогам первой и второй аттестации – 29 баллов;
- по итогам трех аттестаций – 43 балла;
- по итогам промежуточной аттестации – 56 баллов.

Дифференцированная оценка выставляется:

- по результатам экзаменов;
- по учебным дисциплинам трудоемкостью выше трех ЗЕТ;
- по всем видам практик;
- по результатам курсового проектирования (курсовые проекты и работы);
- по результатам защиты итоговой квалификационной работы.

Перевод рейтинговой оценки в дифференцированную осуществляется согласно шкале:

"Отлично" – 85÷100 баллов;

"Хорошо" – 70÷84 баллов;

"Удовлетворительно" – 56÷69 баллов;

"Неудовлетворительно" – 55 баллов и менее

При контроле успеваемости используются формы контроля:

- устный опрос (собеседование);
- тест (в бланковой или компьютерной формах);

- контрольная работа;

- контроль выполнения задания практического задания;

- защита лабораторной работы;

- контроль выполнения индивидуального задания;

- защита курсового проекта (курсовой работы);

- зачет;

- экзамен;

- итоговый междисциплинарный государственный экзамен по специальности;

- контроль выполнения (проверка, рецензирование, нормоконтроль) выпускной квалификационной работы;

- защита выпускной квалификационной работы.

7.1. Фонды оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации

Для оценки качества освоения Основной образовательной программы созданы фонды оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации. Эти фонды позволяют оценить степень сформированности компетенций обучающихся и включают: контрольные вопросы и типовые задания для практических занятий, лабораторных и контрольных работ, зачетов и экзаменов, тесты и компьютерные тестирующие программы, примерную тематику курсовых работ, рефератов.

В разработанном в ДГТУ положении о модульно-рейтинговой системе оценки учебной деятельности студента даны рекомендации преподавателям для проведения текущего контроля успеваемости по дисциплинам (модулям) ООП (заданий для контрольных работ, тематики докладов, рефератов и т.п.), а также методические рекомендации преподавателям по разработке системы оценочных средств и технологий для проведения промежуточной аттестации по дисциплинам (модулям) ООП (в форме зачетов, экзаменов, курсовых работ и практик).

Матрица соответствия компетенций, составных частей ООП и оценочных средств приведена в Приложении 7.

8. Итоговая государственная аттестация выпускников ООП специальности

Итоговая государственная аттестация (ИГА) выпускников специальности 090303.65 - Информационная безопасность автоматизированных систем включает защиту выпускной квалификационной работы и итоговый государственный экзамен. ИГА проводится с целью определения общекультурных и профессиональных компетенций специалиста по защите информации и осуществляется после освоения образовательной программы в полном объеме.

Итоговые аттестационные испытания предназначены для определения профессиональных компетенций специалиста по защите информации, определяющих его подготовленность к решению профессиональных задач, установленных ФГОС, способствующих его устойчивости на рынке труда и продолжению образования в магистратуре.

Аттестационные испытания, входящие в состав итоговой государственной аттестации выпускника, полностью соответствуют программе высшего профессионального образования, которую он освоил за время обучения.

Итоговая государственная аттестация проводится Государственной экзаменационной комиссией (ГЭК) во главе с председателем, утверждаемым Министерством образования и науки РФ. Состав ГЭК утверждается приказом ректора вуза. В состав ГЭК, как правило, вводятся работодатели.

В результате подготовки, защиты выпускной квалификационной работы и сдачи государственного экзамена студент должен:

знать, понимать и решать профессиональные задачи в области научно-исследовательской и производственной деятельности в соответствии со специальностью и выбранной специализацией;

уметь использовать современные методы защиты информации;

владеть приемами осмысления базовой и факультативной информации в области обеспечения защищенности объектов информатизации в условиях

существования угроз в информационной сфере.

8.1. Требования к выпускной квалификационной работе

Выпускная квалификационная работа специалиста по защите информации, представляемая в виде рукописи, является итоговой оценкой деятельности студента и предназначена для получения выпускником опыта постановки и проведения научного исследования. По форме представляет собой углубленную курсовую исследовательскую работу (экспериментальную, расчетную или теоретическую) или проект и должна отражать умение выпускника в составе научного коллектива решать поставленную научную проблему.

Тема выпускной работы определяется выпускающей кафедрой и утверждается заведующим кафедрой. Примерное содержание выпускной работы и общая трудоемкость ее выполнения приведены в методических указаниях по выполнению ВКР.

Защита выпускной работы проводится на заседании ГАК.

Руководитель и рецензент утверждаются кафедрой. Рецензенты назначаются из числа научно-педагогических сотрудников или высококвалифицированных специалистов образовательных, производственных и других учреждений и организаций. В качестве рецензента может выступать представитель работодателей из соответствующих профильных отраслей.

Порядок защиты ВКР устанавливается ученым советом *факультета.* Рекомендуется следующая процедура:

- устное сообщение автора ВКР (5-10 минут);
- вопросы членов ГАК и присутствующих на защите;
- отзыв руководителя ВКР в устной или письменной форме;
- отзыв рецензента ВКР в устной или письменной форме;
- ответ автора ВКР на вопросы и замечания;
- дискуссия;
- заключительное слово автора ВКР.

В своем отзыве руководитель ВКР обязан:

- определить степень самостоятельности студента в выборе темы, поисках

материала, методики его анализа;

- оценить полноту раскрытия темы студентом;
- установить уровень профессиональной подготовки выпускника, освоение им комплекса теоретических и практических знаний, широту научного кругозора студента либо определить степень практической ценности работы;
- оценить работу студента в целом. Рецензент в отзыве о ВКР оценивает:
- степень актуальности и новизны работы;
- четкость формулировок цели и задач исследования;
- степень полноты обзора научной литературы;
- структуру работы и ее правомерность;
- надежность материала исследования — его аутентичность, достаточный объем;
- научный аппарат работы и используемые в ней методы;
- практическую направленность и актуальность проекта.

Рецензия завершается выводом о соответствии работы основным требованиям, предъявляемым к ВКР данного уровня и оценку ВКР.

Оценка за ВКР выставляется ГАК с учетом предложений рецензента и мнения руководителя. При оценке ВКР учитываются:

- содержание работы;
- ее оформление;
- характер защиты.

8.2. Требования к государственному экзамену выпускника по специальности 090303.65 - Информационная безопасность автоматизированных систем

Порядок проведения и программа государственного экзамена определены с учетом требований ФГОС и методических рекомендаций УМО по образованию в области информационной безопасности. Государственный выпускной экзамен призван дать возможность установить уровень образованности, полноту знаний и навыков, приобретенных выпускником в рамках образовательной программы

специальности; уровень интеллектуальных способностей специалиста, его творческие возможности для дальнейшего продолжения образования в аспирантуре или производственной деятельности. В материалах, выносимых на государственный экзамен, представляются основные разделы дисциплин базовой и вариативной части цикла С.3, причем в них, прежде всего, должны найти отражение фундаментальные составляющие этих дисциплин.

Содержание разработанных фондов оценочных средств, позволяющих определить уровень освоения выпускником общекультурных и профессиональных компетенций, приведено в приложении.

Цель итогового государственного экзамена - проверка теоретической и практической подготовленности выпускника к осуществлению профессиональной деятельности и возможному продолжению обучения в аспирантуре.

9. Другие нормативно-методические документы и материалы, обеспечивающие качество подготовки обучающихся по специальности 090303.65 - Информационная безопасность автоматизированных систем

9.1.Система обеспечения качества подготовки специалистов

В ДГТУ внедрена система обеспечения качества подготовки специалистов.

В соответствии с данной системой производится периодический учет и анализ мнений работодателей, выпускников вуза и студентов о качестве образовательного процесса. В результате осуществляется коррекция ООП.

На кафедрах ДГТУ принята практика ежегодной коррекции учебных программ отдельных дисциплин и периодическая корректировка программы в целом.

В качестве примеров улучшения программы подготовки специалистов по результатам контроля выпускников можно привести следующие:

- введение в учебные планы курсов специализации по выбору в соответствии с требованиями заказчиков;

- корректировка рабочих программ курсов учебных планов в соответствии

с требованиями заказчиков;

- постановка циклов лабораторных работ с использованием новых программных пакетов;

- корректировка тематики практических занятий;

- корректировка тематики индивидуальных заданий студентам с учетом реальных задач, формулируемых предприятиями и организациями;

- корректировка тематики курсовых проектов с учетом реальных задач, формулируемых предприятиями и организациями;

- корректировка тематики плановой научно-исследовательской работы студентов с учетом реальных задач, формулируемых предприятиями и организациями;

- расширение мест организации производственной практики за счет ведущих предприятий и организаций региона;

- корректировка тем выпускных работ с учетом реальных задач, формулируемых предприятиями и организациями.

Потенциальными потребителями специалистов в области информационной безопасности в Республике Дагестан являются: министерства и ведомства республики, в т.ч. силовые; муниципальные органы власти; предприятия оборонно-промышленного комплекса; банковские и коммерческие структуры; Управление Федерального Казначейства по РД; отделение Пенсионного Фонда РФ по РД, радио- и телевещательные компании.

С целью обеспечения компетентности преподавательского состава в ДГТУ принята практика контроля занятий заведующим кафедрой, взаимное посещение занятий преподавателями кафедры, а также анкетирование студентов по оценке преподавателей.

9.2. Система менеджмента качества и учет интересов потребителей

В соответствии с требованиями международного стандарта ИСО 9001:2008 в области обеспечения качества подготовки специалистов университет в целом и факультет КТВТиЭ ДГТУ, в частности, руководствуются следующими документами системы менеджмента качества:

- инструкция и информационная карта процесса «Управление образовательной средой»;

- инструкция и информационная карта процесса «Воспитательная и внеучебная работа с обучающимися»,

- инструкция и информационная карта процесса «Реализация основных образовательных программ»;

- инструкция и информационная карта процесса «Проектирование и разработка образовательных программ ВПО» и др.

В целях оценки качества образовательных услуг университетом проводится мониторинг и систематические самообследования, регламентированные следующими внутренними нормативными документами:

- Положение о консолидированном рейтинге факультетов ДГТУ;

- Положение о мониторинге оценки качества образовательных услуг участниками образовательного процесса ДГТУ и работодателями;

В ходе самообследования ДГТУ проверяет себя по ряду критериев:

- состояние материально-технической базы;

- качество профессорско-преподавательского состава;

- научно-методическая обеспеченность учебного заведения;

- сведения о карьерном росте выпускников и их востребованности на рынке труда.

Методическими материалами, обеспечивающими качество подготовки обучающихся служат паспорта компетенций для всех обязательных компетенций из ФГОС ВПО, включающие определение компетенций, ее структуру, уровни ее сформированности в вузе по окончании освоения ООП, признаки (дескрипторы) уровней сформированности компетенций, разработанные на основе ФГОС ВПО и утвержденные на учебно-методическом совете факультета.

Для эффективности управления качеством научно-образовательной деятельности в ДГТУ имеются различные информационные системы, в частности, ИИК, цифровой кампус, web-портал научно-технической библиотеки

ДГТУ, Интернет-страницы выпускающих и обеспечивающих кафедр.

Применение данных инструментариев позволяет описать систему внешней оценки качества реализации ООП с учетом и анализом мнений работодателей, выпускников вуза и других субъектов образовательного процесса.

Основным принципом, заложенным в систему менеджмента качества, является принцип ориентации на потребителя. Потребителями образовательной программы являются студенты и их родители, работодатели, государство. На основании пожеланий потребителей в образовательную программу могут вноситься оперативные изменения: пересматриваться и изменяться учебный план, вводиться новые учебные дисциплины, изменяться форма их изучения. При необходимости по заказу потребителей студенты могут обучаться по индивидуальным учебным планам, разработанным по заказу и с учетом интересов конкретных потребителей (промышленных предприятий, организаций, студентов).

Разработчик программы:

Зав. кафедрой ПОВТиАС, д.т.н., доцент _____ А.Г. Мустафаев

Приложение

Утвержден
приказом Министерства образования
и науки Российской Федерации
от «17» января 2011 г. № 80

ФЕДЕРАЛЬНЫЙ ГОСУДАРСТВЕННЫЙ ОБРАЗОВАТЕЛЬНЫЙ СТАНДАРТ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

по направлению подготовки (специальности)

090303 Информационная безопасность автоматизированных систем

(квалификация (степень) «специалист»)

I. ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1. Настоящий федеральный государственный образовательный стандарт высшего профессионального образования (ФГОС ВПО) представляет собой совокупность требований, обязательных при реализации основных образовательных программ подготовки специалистов по направлению подготовки (специальности) **090303 Информационная безопасность автоматизированных систем** образовательными учреждениями высшего профессионального образования (высшими учебными заведениями, вузами), имеющими государственную аккредитацию, на территории Российской Федерации.

1.2. Право на реализацию основных образовательных программ высшее учебное заведение имеет только при наличии соответствующей лицензии, выданной уполномоченным федеральным органом исполнительной власти.

II. ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ

В настоящем стандарте используются следующие сокращения:

ВПО - высшее профессиональное образование;

ООП - основная образовательная программа;

ОК - общекультурные компетенции;

ПК - профессиональные компетенции;

ПСК - профессионально-специализированные компетенции;

УЦ ООП - учебный цикл основной образовательной программы;

ФГОС ВПО - федеральный государственный образовательный стандарт высшего профессионального образования.

III. ХАРАКТЕРИСТИКА НАПРАВЛЕНИЯ ПОДГОТОВКИ (СПЕЦИАЛЬНОСТИ)

Нормативный срок, общая трудоемкость освоения ООП (в зачетных единицах)* и соответствующая квалификация (степень) приведены в таблице 1.

Таблица 1

Сроки, трудоемкость освоения ООП и квалификация (степень) выпускников

Наименование ООП	Квалификация (степень)		Нормативный срок освоения ООП (для очной формы обучения), включая каникулы, предоставляемые после прохождения итоговой государственной аттестации	Трудоемкость (в зачетных единицах)
	Код в соответствии с принятой классификацией ООП	Наименование		
ООП подготовки специалиста	65	специалист	5 лет	300**

*Одна зачетная единица соответствует 36 академическим часам.

**Трудоемкость ООП подготовки специалиста по очной форме обучения в среднем за учебный год равна 60 зачетным единицам.

По данной ООП подготовки специалиста обучение в форме очно-заочной (вечерней), заочной и экстерната не допускается.

IV. ХАРАКТЕРИСТИКА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ СПЕЦИАЛИСТОВ

4.1. Область профессиональной деятельности специалистов включает: сферы науки, техники и технологии, охватывающие совокупность проблем, связанных с обеспечением информационной безопасности автоматизированных систем в условиях существования угроз в информационной сфере.

4.2. Объектами профессиональной деятельности специалистов являются: автоматизированные системы, функционирующие в условиях существования угроз в информационной сфере и обладающие информационно-технологическими ресурсами, подлежащими защите; информационные технологии, формирующие информационную инфраструктуру в условиях существования угроз в информационной сфере и задействующие информационно-технологические ресурсы, подлежащие защите; технологии обеспечения информационной безопасности автоматизированных систем; системы управления информационной безопасностью автоматизированных систем.

4.3. Специалист по направлению подготовки (специальности) **090303 Информационная безопасность автоматизированных систем** готовится к следующим видам профессиональной деятельности:

научно-исследовательская;

проектно-конструкторская;

контрольно-аналитическая;

организационно-управленческая;

эксплуатационная.

Конкретные виды профессиональной деятельности, к которым в основном готовится специалист, определяются высшим учебным заведением совместно с обучающимися, научно-педагогическими работниками высшего учебного заведения и объединениями работодателей.

По окончании обучения по направлению подготовки (специальности) **090303 Информационная безопасность автоматизированных систем,** наряду с квалификацией (степенью) «специалист» присваивается специальное звание «специалист по защите информации».

4.4. Специалист по направлению подготовки (специальности) **090303 Информационная безопасность автоматизированных систем** должен решать следующие профессиональные задачи в соответствии с видами профессиональной деятельности:

научно-исследовательская деятельность:

сбор, обработка, анализ и систематизация научно-технической информации, отечественного и зарубежного опыта по проблемам информационной безопасности автоматизированных систем;

подготовка научно-технических отчетов, обзоров, публикаций по результатам выполненных исследований;

моделирование и исследование защищенных автоматизированных систем, анализ их уязвимостей и эффективности средств и способов защиты;

анализ безопасности информационных технологий, реализуемых в автоматизированных системах;

разработка эффективных решений по обеспечению информационной безопасности автоматизированных систем;

проектно-конструкторская деятельность:

сбор и анализ исходных данных для проектирования систем защиты информации;

разработка политик информационной безопасности автоматизированных систем;

разработка защищенных автоматизированных систем по профилю профессиональной деятельности, обоснование выбора способов и средств защиты информационно-технологических ресурсов автоматизированных систем;

выполнение проектов по созданию программ, комплексов программ, программно-аппаратных средств, баз данных, компьютерных сетей для защищенных автоматизированных систем;

разработка системы управления информационной безопасностью автоматизированных систем;

контрольно-аналитическая:

контроль работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации;

экспериментально-исследовательские работы при сертификации средств защиты автоматизированных систем;

экспериментально-исследовательские работы при аттестации автоматизированных систем;

инструментальный мониторинг защищенности автоматизированных систем;

организационно-управленческая деятельность:

организация работы коллектива, принятие управленческих решений в условиях спектра мнений, определение порядка выполнения работ;

разработка предложений по совершенствованию и повышению эффективности принятых мер по обеспечению информационной безопасности автоматизированных систем;

организация работ по выполнению требований защиты информации ограниченного доступа;

методическое и организационное обеспечение информационной безопасности автоматизированных систем;

организация работ по созданию, внедрению, эксплуатации и сопровождению защищенных автоматизированных систем;

контроль реализации политики информационной безопасности;

эксплуатационная деятельность:

реализация информационных технологий в сфере профессиональной деятельности с использованием защищенных автоматизированных систем;

администрирование подсистем информационной безопасности автоматизированных систем;

мониторинг информационной безопасности автоматизированных систем;

управление информационной безопасностью автоматизированных систем;

обеспечение восстановления работоспособности систем защиты информации при возникновении нештатных ситуаций.

V. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ОСНОВНЫХ ОБРАЗОВАТЕЛЬНЫХ ПРОГРАММ ПОДГОТОВКИ СПЕЦИАЛИСТА

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

способностью действовать в соответствии с Конституцией Российской Федерации, исполнять свой гражданский и профессиональный долг, руководствуясь принципами законности и патриотизма (ОК-1);

способностью осуществлять свою деятельность в различных сферах общественной жизни с учетом принятых в обществе морально-нравственных и правовых норм, соблюдать принципы профессиональной этики (ОК-2);

способностью анализировать социально значимые явления и процессы, в том числе политического и экономического характера, мировоззренческие и философские проблемы, применять основные

положения и методы гуманитарных, социальных и экономических наук при решении социальных и профессиональных задач (ОК-3);

способностью понимать движущие силы и закономерности исторического процесса, роль личности в истории, политической организации общества, способностью уважительно и бережно относиться к историческому наследию, толерантно воспринимать социальные и культурные различия (ОК-4);

способностью понимать социальную значимость своей будущей профессии, цели и смысл государственной службы, обладать высокой мотивацией к профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства (ОК-5);

способностью к работе в коллективе, кооперации с коллегами, способностью в качестве руководителя подразделения, лидера группы сотрудников формировать цели команды, принимать организационно-управленческие решения в нестандартных ситуациях и нести за них ответственность, предупреждать и конструктивно разрешать конфликтные ситуации в процессе профессиональной деятельности (ОК-6);

способностью логически верно, аргументировано и ясно строить устную и письменную речь на русском языке, готовить и редактировать тексты профессионального назначения, публично представлять собственные и известные научные результаты, вести дискуссии (ОК-7);

способностью к письменной и устной деловой коммуникации, к чтению и переводу текстов по профессиональной тематике на одном из иностранных языков (ОК-8);

способностью к логическому мышлению, обобщению, анализу, критическому осмыслению информации, систематизации, прогнозированию,

постановке исследовательских задач и выбору путей их решения на основании принципов научного познания (ОК-9);

способностью самостоятельно применять методы и средства познания, обучения и самоконтроля для приобретения новых знаний и умений, в том числе в новых областях, непосредственно не связанных со сферой профессиональной деятельности, развития социальных и профессиональных компетенций, к изменению вида своей профессиональной деятельности (ОК-10);

способностью к воспитательной и образовательной деятельности (ОК-11);

способностью самостоятельно применять методы физического воспитания для повышения адаптационных резервов организма и укрепления здоровья, достижения должного уровня физической подготовленности в целях обеспечения полноценной социальной и профессиональной деятельности (ОК-12).

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

общепрофессиональными:

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

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

способностью использовать языки, системы и инструментальные средства программирования в профессиональной деятельности (ПК-3);

способностью понимать сущность и значение информации в развитии современного общества, применять достижения современных

информационных технологий для поиска и обработки больших объемов информации по профилю деятельности в глобальных компьютерных системах, сетях, в библиотечных фондах и в иных источниках информации (ПК-4);

способностью применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ПК-5);

способностью использовать нормативные правовые акты в своей профессиональной деятельности (ПК- 6);

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

способностью к освоению новых образцов программных, технических средств и информационных технологий (ПК-8);

в научно - исследовательской деятельности:

способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере своей профессиональной деятельности (ПК-9);

способностью применять современные методы исследования с использованием компьютерных технологий (ПК-10);

способностью разрабатывать и исследовать модели автоматизированных систем (ПК-11);

способностью проводить анализ защищенности автоматизированных систем (ПК-12);

способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы (ПК-13);

способностью проводить анализ рисков информационной безопасности автоматизированной системы (ПК-14);

способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем (ПК-15);

способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ (ПК-16);

в проектно-конструкторской деятельности:

способностью проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем (ПК-17);

способностью участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности (ПК-18);

способностью участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности (ПК-19);

способностью разрабатывать политики информационной безопасности автоматизированных систем (ПК-20);

способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы (ПК-21);

способностью участвовать в проектировании средств защиты информации и средств контроля защищенности автоматизированной системы (ПК-22);

в контрольно-аналитической деятельности:

способностью проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-23);

способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты автоматизированных систем (ПК-24);

способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных требований по защите информации (ПК-25);

способностью проводить инструментальный мониторинг защищенности автоматизированных систем (ПК-26);

в организационно-управленческой деятельности:

способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности (ПК-27);

способностью разрабатывать оперативные планы работы первичных подразделений (ПК-28);

способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы (ПК-29);

способностью организовать эксплуатацию автоматизированной системы с учетом требований информационной безопасности (ПК-30);

способностью разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, а также положений, инструкций и других организационно-распорядительных документов в сфере профессиональной деятельности (ПК-31);

способностью проводить анализ особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите (ПК-32);

способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации (ПК-33);

способностью формировать комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной системы (ПК-34);

в эксплуатационной деятельности:

способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности (ПК-35);

способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы (ПК-36);

способностью администрировать подсистему информационной безопасности автоматизированной системы (ПК-37);

способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы (ПК-38);

способностью управлять информационной безопасностью автоматизированной системы (ПК-39);

способностью обеспечить восстановление работоспособности систем защиты информации при возникновении нештатных ситуаций (ПК-40).

Специализация № 1 «Автоматизированные информационные системы специального назначения».*

Специализация № 2 «Высокопроизводительные вычислительные системы специального назначения».*

---

* В соответствии с п. 7.1 настоящего стандарта требования к специализации определяются вузом.

Специализация № 3 «Информационная безопасность автоматизированных систем критически важных объектов»:

способностью проводить оценку эффективности средств защиты информации, использующихся на критически важных объектах и в автоматизированных системах критически важных объектов (ПСК-3.1);

способностью участвовать в разработке средств защиты информации, использующихся на критически важных объектах и в автоматизированных системах критически важных объектов (ПСК-3.2);

способностью применять современную нормативную базу, регламентирующую деятельность критически важных объектов и обеспечение информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов (ПСК-3.3);

способностью разрабатывать технические регламенты для различных видов деятельности по обеспечению информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов (ПСК-3.4);

способностью проектировать, внедрять и использовать системы мониторинга средств защиты информации, функционирующих на критически важных объектах и в автоматизированных системах критически важных объектов (ПСК-3.5);

способностью восстанавливать работоспособность средств защиты информации, функционирующих на критически важных объектах и в автоматизированных системах критически важных объектов (ПСК-3.6).

Специализация № 4 «Безопасность открытых информационных систем»:

способностью проводить анализ и исследовать модели защищенности открытых информационных систем (ПСК-4.1);

способностью участвовать в разработке компонентов открытых информационных систем (ПСК-4.2);

способностью обеспечить эффективное применение информационно-технологических ресурсов открытых информационных систем с учетом нормативных требований по защите информации (ПСК-4.3);

способностью разрабатывать и реализовывать политики информационной безопасности открытых информационных систем (ПСК-4.4);

способностью участвовать в проектировании и эксплуатации системы управления информационной безопасностью открытой информационной системы (ПСК-4.5);

способностью проводить инструментальный мониторинг защищенности открытых информационных систем (ПСК-4.6);

способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью открытой информационной системы (ПСК-4.7);

способностью формировать и эффективно применять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности открытых информационных систем (ПСК-4.8).

Специализация № 5 «Информационная безопасность автоматизированных банковских систем»:

способностью проводить анализ и исследовать модели автоматизированных банковских систем (ПСК-5.1);

способностью на практике применять стандарты, относящиеся к обеспечению информационной безопасности автоматизированных банковских систем (ПСК-5.2);

способностью на практике применять криптографические протоколы и стандарты при обеспечении информационной безопасности автоматизированных банковских систем (ПСК-5.3);

способностью проводить синтез и анализ проектных решений по обеспечению информационной безопасности автоматизированных банковских систем (ПСК-5.4);

способностью обеспечивать эффективное применение информационно-технологических ресурсов автоматизированных банковских систем с учетом нормативных требований по защите информации (ПСК-5.5);

способностью разрабатывать и реализовывать политики информационной безопасности автоматизированных банковских систем (ПСК-5.6);

способностью участвовать в проектировании и эксплуатации системы управления информационной безопасностью автоматизированных банковских систем (ПСК-5.7);

способностью проводить инструментальный мониторинг защищенности автоматизированных банковских систем (ПСК-5.8);

способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной банковской системы (ПСК-5.9);

способностью формировать и эффективно применять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной банковской системы (ПСК-5.10).

Специализация № 6 «Защищенные автоматизированные системы управления»:

способностью разрабатывать алгоритмы управления для защищенных автоматизированных систем управления на основе методов теории управления (ПСК-6.1);

способностью выбирать методы и разрабатывать алгоритмы принятия решений в защищенных автоматизированных системах управления (ПСК-6.2);

способностью выявлять режимы работы элементов защищенных автоматизированных систем управления и внешние воздействия на них, способствующие увеличению риска утечки информации в различных физических полях (ПСК-6.3);

способностью участвовать в разработке подсистем мониторинга информационной безопасности защищенных автоматизированных систем управления (ПСК-6.4);

способностью планировать, реализовывать, оценивать и корректировать основные процессы управления информационной безопасностью защищенных автоматизированных систем управления и организаций (ПСК-6.5);

способностью применять современные технологии проектирования защищенных автоматизированных систем управления (ПСК-6.6);

способностью участвовать в разработке и оценке соответствия средств защиты информации подсистем обеспечения информационной безопасности защищенных автоматизированных систем управления нормативным требованиям по защите информации (ПСК-6.7).

Специализация № 7 «Обеспечение информационной безопасности распределенных информационных систем»:

способностью разрабатывать и исследовать модели информационно-технологических ресурсов в распределенных информационных системах (ПСК-7.1);

способностью разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах (ПСК-7.2);

способностью проводить анализ рисков информационной безопасности в распределенных информационных системах (ПСК-7.3);

способностью разрабатывать и руководить разработкой политики безопасности распределенных информационных систем (ПСК-7.4);

способностью проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем (ПСК-7.5);

способностью проводить удаленное администрирование операционных систем в распределенных информационных системах (ПСК-7.6);

способностью проводить удаленное администрирование систем баз данных в распределенных информационных системах (ПСК-7.7);

способностью координировать деятельность подразделений и специалистов по защите информации на предприятии, в учреждении, организации (ПСК-7.8);

способностью применять криптографические протоколы для передачи и хранения данных в распределенных информационных системах (ПСК-7.9).

Специализация № 8 «Анализ безопасности информационных систем»:

способностью использовать языки, системы, инструментальные программные и аппаратные средства для моделирования информационных систем и испытаний систем защиты (ПСК-8.1);

способностью разрабатывать методики и тесты для анализа степени защищенности информационной системы, соответствия нормативным требованиям по защите информации (ПСК-8.2);

способностью применять инструментарий анализа безопасности программного обеспечения (ПСК-8.3);

способностью применять методы дизассемблирования программ и методы восстановления алгоритма программы по ее дизассемблированному коду (ПСК-8.4);

способностью принимать участие в проведении исследований и испытаний защищенных информационных систем (ПСК-8.5);

способностью участвовать в сертификационных испытаниях по существующим требованиям (ПСК-8.6).

Специализация № 9 «Создание автоматизированных систем в защищенном исполнении»:

способностью разрабатывать модели угроз и модели нарушителей информационной безопасности процессов создания и эксплуатации автоматизированных систем в защищенном исполнении (ПСК-9.1);

способностью принимать участие в разработке, реализации и управлении процессами создания и эксплуатации автоматизированных систем в защищенном исполнении на всех стадиях и этапах их жизненного цикла (ПСК-9.2);

способностью рационально выбирать методы и средства для реализации процессов создания и эксплуатации автоматизированных систем в защищенном исполнении (ПСК-9.3);

способностью применять современные технологии проектирования автоматизированных систем в защищенном исполнении (ПСК-9.4);

способностью применять нормативные правовые акты, руководящие и методические документы, регламентирующие процессы создания и эксплуатации автоматизированных систем в защищенном исполнении на различных стадиях их жизненного цикла (ПСК-9.5);

способностью проводить анализ достаточности мер по обеспечению информационной безопасности процессов создания и эксплуатации автоматизированных систем в защищенном исполнении (ПСК-9.6).

Специализация № 10 «Информационная безопасность автоматизированных систем на транспорте»:

способностью участвовать в разработке защищенных автоматизированных, информационно-управляющих и информационно-логистических систем транспорта (ПСК-10.1);

способностью применять программные, программно-аппаратные и технические методы и средства защиты информации в распределенных

автоматизированных, информационно-управляющих и информационно-логистических системах транспорта (ПСК-10.2);

способностью разрабатывать предложения по совершенствованию мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности в распределенных автоматизированных, информационно-управляющих и информационно-логистических системах транспорта (ПСК-10.3);

способностью проводить оценку эффективности средств защиты информации, использующихся в автоматизированных, информационно-управляющих и информационно-логистических системах транспорта (ПСК-10.4);

способностью разрабатывать политику безопасности распределенных автоматизированных, информационно-управляющих и информационно-логистических систем транспорта (ПСК-10.5);

способностью разрабатывать предложения по совершенствованию системы аудита и управления информационной безопасностью автоматизированных и информационно-управляющих систем транспорта (ПСК-10.6);

способностью осуществлять мониторинг и аудит уровня защищенности, оценку соответствия и аттестацию распределенных автоматизированных, информационно-управляющих и информационно-логистических систем транспорта с учетом нормативных требований по защите информации (ПСК-10.7);

способностью осуществлять рациональный выбор элементной базы обеспечения информационной безопасности распределенных автоматизированных, информационно-управляющих и информационно-логистических систем транспорта (ПСК-10.8);

способностью обеспечить эффективное применение средств защиты технологического электронного документооборота и технического документоведения на транспорте (ПСК-10.9);

способностью выявлять и прогнозировать угрозы информационной безопасности автоматизированных и информационно-управляющих систем транспорта, разрабатывать меры противодействия (ПСК-10.10).

VI. ТРЕБОВАНИЯ К СТРУКТУРЕ ОСНОВНЫХ ОБРАЗОВАТЕЛЬНЫХ ПРОГРАММ ПОДГОТОВКИ СПЕЦИАЛИСТА

6.1. ООП подготовки специалиста предусматривает изучение следующих учебных циклов (таблица 2):

гуманитарный, социальный и экономический цикл;

математический и естественнонаучный цикл;

профессиональный цикл;

и разделов:

физическая культура

учебная и производственная практики, научно-исследовательская работа;

итоговая государственная аттестация.

6.2. Каждый учебный цикл имеет базовую (обязательную) часть и вариативную, устанавливаемую вузом. Вариативная часть дает возможность расширения и (или) углубления знаний, умений и навыков, определяемых содержанием базовых (обязательных) дисциплин (модулей) и дисциплин специализаций, позволяет обучающемуся получить углубленные знания и навыки для успешной профессиональной деятельности и (или) для продолжения дальнейшего обучения по программам послевузовского профессионального образования (аспирантура, адъюнктура).

6.3. Базовая (обязательная) часть цикла «Гуманитарный, социальный и экономический цикл» должна предусматривать изучение следующих

обязательных дисциплин: «История Отечества», «Философия», «Иностранный язык».

Базовая (обязательная) часть профессионального цикла должна предусматривать изучение всех дисциплин, указанных в структуре ООП подготовки специалиста.

Таблица 2

Структура ООП подготовки специалиста

Код УЦ ООП	Учебные циклы (разделы) и проектируемые результаты их освоения	Трудоемкость (Зачетные единицы)[1]	Перечень дисциплин для разработки программ (примерных), а также учебников и учебных пособий	Коды формируемых компетенций
С.1	**Гуманитарный, социальный и экономический цикл**	**32-39**		
	Базовая часть В результате изучения базовой части цикла обучающийся должен: **знать:** – содержание и взаимосвязь основных принципов, законов, понятий и категорий гуманитарных, социальных и экономических наук; – основные этапы развития философской мысли, основную проблематику и структуру философского знания; – основные закономерности исторического процесса, этапы исторического развития России, место и роль России в истории человечества и в современном мире; – лексический и грамматический минимум в объеме, необходимом для работы с текстами	**24-29**[3]	Философия История Отечества Иностранный язык Правоведение Экономика Основы управленческой деятельности	ОК-1 ОК-2 ОК-3 ОК-4 ОК-5 ОК-6 ОК-7 ОК-8 ОК-9 ОК-10 ОК-11 ПК-5 ПК-6 ПК-9 ПК-27 ПК-28 ПК-31 ПК-33

Продолжение цикла С.1				
	профессиональной направленности и осуществления коммуникации на иностранном языке; – основные экономические теории, категории и закономерности, методы анализа экономических явлений и процессов; - основы экономической и финансовой деятельности отрасли и ее структурных подразделений, методику оценки хозяйственной, деятельности (применительно к отрасли обеспечения информационной безопасности); – основы права и законодательства России, основы конституционного строя Российской Федерации, характеристику основных отраслей российского права, правовые основы обеспечения национальной безопасности Российской Федерации; – научные основы, цели, принципы, методы и технологии управленческой деятельности; **уметь:** – использовать принципы, законы и методы гуманитарных, социальных и экономических наук для решения профессиональных задач; – анализировать мировоззренческие, социально и личностно значимые философские проблемы; – анализировать современные общественные процессы, опираясь на принципы историзма и научной объективности; – читать и переводить научно-техническую литературу на иностранном языке по профессиональной тематике, правильно употреблять терминологическую лексику в профессиональной речи; – анализировать экономические показатели деятельности подразделения; – использовать в практической деятельности правовые знания,			

Продолжение цикла С.1				
	анализировать основные правовые акты, давать правовую оценку информации, используемой в профессиональной деятельности; – работать в коллективе, принимать управленческие решения и оценивать их эффективность; **владеть:** – основными методами научного познания; – иностранным языком в объеме, необходимом для получения и изложения информации по профессиональной тематике, навыками общения на иностранном языке; – навыками письменного аргументированного изложения собственной точки зрения; – навыками публичной речи, аргументации, ведения дискуссии и полемики; – навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности; – навыками выбора, обоснования, реализации и контроля результатов управленческого решения.			
	Вариативная часть (знания, умения, навыки определяются ООП вуза)	**8-10**		
С.2	**Математический и естественнонаучный цикл**	**74-83**		
	Базовая часть В результате изучения базовой части цикла обучающийся должен: **знать:** – основные понятия и задачи векторной алгебры и аналитической геометрии; – основные свойства алгебраических структур; – основы линейной алгебры над произвольными полями; – основные положения теории пределов функций, теории рядов; – основные теоремы дифференциального и интегрального исчисления функций одного и нескольких переменных;	**65-69**[3]	Алгебра и геометрия Математический анализ Дискретная математика Теория вероятностей и математическая статистика Математическая логика и теория алгоритмов	ОК-5 ОК-7 ОК-9 ОК-10 ПК-1 ПК-2 ПК-4 ПК-5 ПК-8 ПК-9 ПК-10 ПК-17 ПК-18 ПК-19 ПК-22 ПК-23 ПК-24

Продолжение цикла С.2			
– основные понятия и методы теории вероятностей, теории случайных процессов и математической статистики; – основы комбинаторного анализа; – основные понятия теории автоматов; – основные дискретные структуры: конечные автоматы, грамматики, графы, комбинаторные структуры; – методы перечисления для основных дискретных структур; – основные принципы математической логики; – формализации понятия алгоритма: машины Тьюринга, рекурсивные функции; – основные понятия теории сложности алгоритмов; – основные понятия теории информации и кодирования: энтропия, взаимная информация, источники сообщений, каналы связи, коды; – основные результаты о кодировании при наличии и отсутствии шума; – основные методы оптимального кодирования источников информации и помехоустойчивого кодирования каналов связи; – основные законы механики; – основные законы термодинамики и молекулярной физики; – основные законы электричества и магнетизма; – основы теории колебаний и волн, оптики; – основы квантовой физики и физики твёрдого тела; – физические явления и эффекты, используемые при обеспечении информационной безопасности автоматизированных систем; – основные понятия информатики; – формы и способы представления данных в персональном компьютере; – состав, назначение функциональных компонентов и		Теория информации Информатика Физика	ПК-25 ПК-26

Продолжение цикла С.2				
	программного обеспечения персонального компьютера; – классификацию современных компьютерных систем; – типовые структуры и принципы организации компьютерных сетей; **уметь:** – строить и изучать математические модели конкретных явлений и процессов для решения расчетных и исследовательских задач; – определять возможности применения теоретических положений и методов математических дисциплин для постановки и решения конкретных прикладных задач; – решать основные задачи векторной алгебры и аналитической геометрии; – решать основные задачи на вычисление пределов функций, дифференцирование и интегрирование, на разложение функций в ряды; – оперировать с числовыми многочленами, матрицами; – решать основные задачи линейной алгебры, системы линейных уравнений над полями; – применять стандартные методы и модели к решению типовых теоретико-вероятностных и статистических задач; – пользоваться расчетными формулами, таблицами, компьютерными программами при решении математических задач; – применять стандартные методы дискретной математики и теории автоматов для решения профессиональных задач; – оценивать сложность алгоритмов и вычислений; – вычислять теоретико-информационные характеристики источников сообщений и каналов связи; – решать типовые задачи кодирования и декодирования;			

Продолжение цикла С.2			
– строить математические модели физических явлений и процессов; – решать типовые прикладные физические задачи; – анализировать и применять физические явления и эффекты для решения практических задач обеспечения информационной безопасности; – применять типовые программные средства сервисного назначения (средства восстановления системы после сбоев, очистки и дефрагментации диска); – пользоваться сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети Интернет; **владеть:** – навыками использования стандартных методов и моделей математического анализа и их применения к решению прикладных задач; – навыками использования методов аналитической геометрии и векторной алгебры в смежных дисциплинах и физике; – методами линейной алгебры; – навыками использования стандартных теоретико-вероятностных и статистических методов при решении прикладных задач; – навыками построения дискретных моделей при решении профессиональных задач; – способами оценки сложности работы алгоритмов; – основами построения математических моделей систем передачи информации; – навыками применения математического аппарата для решения прикладных теоретико-информационных задач; – навыками пользования библиотеками прикладных программ для решения прикладных			

Продолжение цикла С.2			
математических задач; – методами теоретического исследования физических явлений и процессов; – навыками проведения физического эксперимента и обработки его результатов; – навыками работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов); – навыками обеспечения безопасности информации с помощью типовых программных средств (антивирусов, архиваторов, стандартных сетевых средств обмена информацией).			
1. Специализация «**Автоматизированные информационные системы специального назначения**»[2]	**7-10**		
2. Специализация «**Высокопроизводительные вычислительные системы специального назначения**»[2]	**7-10**		
3. Специализация «**Информационная безопасность автоматизированных систем критически важных объектов**». С целью получения данной специализации при изучении базовой части цикла обучающийся должен: **знать:** – основы теории погрешностей измерений, методы обработки результатов измерений; – способы нормирования и формы задания метрологических характеристик средств измерений; – основные нормативные правовые акты в области метрологии; – цели и методы сертификации; – принципы, методы измерений радиотехнических величин и структурные схемы радиоизмерительных приборов; – принципы построения и структуру автоматизированных средств	**7-10**	Теория функций комплексного переменного Метрология и электро-радиоизмерения Основы радиотехники Антенно-фидерные устройства Теория надежности	ПСК-3.1 ПСК-3.2 ПСК-3.3 ПСК-3.4 ПСК-3.5 ПСК-3.6

Продолжение цикла С.2			
измерений и контроля; – методы статистической радиотехники; – основные тенденции развития теории и техники антенн и сверхвысокочастотных устройств; – методы расчета и измерения параметров основных линий передачи сверхвысокочастотного диапазона; – основные понятия теории надежности; – способы расчета оценочных показателей надежности аппаратных и программных средств автоматизированных систем обработки информации и управления; – способы повышения надежности систем; **уметь:** – дифференцировать функции комплексного переменного, строить конформные отображения простейших областей, вычислять комплексные интегралы, раскладывать функции в ряд Тейлора и ряд Лорана, а также вычислять вычеты функций; – определять структуру оптимальных устройств обработки сигналов информационных радиотехнических систем и оценивать эффективность их работы; – определять оптимальные алгоритмы работы, оптимальную структуру и характеристики различных радиотехнических устройств; – использовать современные программные средства для проектирования технологической документации; – выбирать и оценивать различные структуры систем с точки зрения надежности; **владеть:** – методами комплексного анализа для вычисления определенных и			

Продолжение цикла С.2				
	несобственных интегралов и решения других задач алгебры и анализа; – методами проектирования систем, удовлетворяющих заданным требованиям надежности.			
	4. Специализация **«Безопасность открытых информационных систем».** С целью получения данной специализации при изучении базовой части цикла обучающийся должен: **знать:** – базовые вопросы построения открытых информационных систем; – основные криптографические протоколы и стандарты; – основные стандарты построения и взаимодействия открытых систем; **уметь:** – применять на практике стандарты, относящиеся к открытым информационным системам; **владеть:** – методикой анализа структуры открытых информационных систем.	**7-10**	Открытые информационные системы Криптографические протоколы и стандарты	ПСК-4.1 ПСК-4.2
	5. Специализация **«Информационная безопасность автоматизированных банковских систем».** С целью получения данной специализации при изучении базовой части цикла обучающийся должен: **знать:** – базовые вопросы построения автоматизированных банковских систем; – основные стандарты, относящиеся к обеспечению информационной безопасности автоматизированных банковских систем; – основы обеспечения катастрофоустойчивости автоматизированных банковских систем; – основные криптографические протоколы и стандарты, используемые в автоматизированных банковских системах;	**7-10**	Автоматизированные банковские системы Катастрофоустойчивость автоматизированных банковских систем Криптография в банковском деле	ПСК-5.1 ПСК-5.2 ПСК-5.3

Продолжение цикла С.2			
уметь: – применять на практике стандарты, относящиеся к обеспечению информационной безопасности банковской организации; **владеть:** – методикой анализа структуры автоматизированной банковской системы.			
6. Специализация **«Защищенные автоматизированные системы управления»**. С целью получения данной специализации при изучении базовой части цикла обучающийся должен: **знать:** – основы системного подхода к управлению; – физические явления возникновения побочных сигналов в различных физических полях; – связь информативных признаков с параметрами побочных сигналов; – спектрально-энергетические характеристики информативных сигналов в физических полях любой природы; – основные понятия теории конфликтов; – основные понятия теории игр; – основные понятия теории принятия решений; – основные методы срыва процесса своевременного принятия решения; – основные методы навязывания принятия ложного решения; – основные методы принятия решений в условиях: неопределенности, неполноты сведений, навязывания ложной информации, дефицита времени и вычислительных ресурсов; **уметь:** – выбирать и описывать тип системы управления при решении специализированных прикладных профессиональных задач; – применять измерительное	**7-10**	Основы теории управления Физические основы защиты информации Теория принятия решений в условиях информационных конфликтов	ПСК – 6.1 ПСК – 6.2 ПСК – 6.3

Продолжение цикла С.2			
оборудование для измерения параметров информативных сигналов в физических полях; – выбирать методы и модели принятия решений в защищенных автоматизированных системах управления; – разрабатывать алгоритмы принятия решений для заданных условий эксплуатации защищенных автоматизированных систем управления; – выявлять уязвимости различных методов и алгоритмов принятия решений для заданных условий эксплуатации защищенных автоматизированных систем управления; **владеть:** – навыками анализа и синтеза систем управления; – навыками выбора и оптимизации вида базисных функций, соответствующих обрабатываемым сигналам и элементной базе; – навыками оценки технических характеристик информативных сигналов в различных физических полях; – навыками разработки алгоритмов защиты от принятия несвоевременных и ложных решений; – навыками оценки вычислительной сложности реализации выбранных или разработанных алгоритмов принятия решений.			
7. Специализация **«Обеспечение информационной безопасности распределенных информационных систем».** С целью получения данной специализации при изучении базовой части цикла обучающийся должен: **знать:** – общую постановку задач математического программирования, динамического программирования, сетевого планирования, теории игр;	**7-10**	Исследование операций и теории игр Теория графов и ее приложения	ПСК-7.1 ПСК-7.2 ПСК-7.4 ПСК-7.5 ПСК-7.9

Продолжение цикла С.2			
- универсальные приемы исследования оптимизационных проблем при различной степени неопределенности условий; – структуру представления конечных групп; **уметь:** – формировать множество альтернативных решений, ставить цель и выбрать оценочный критерий оптимальности, сформулировать ограничения на управляемые переменные, связанные со спецификой моделируемой системы; – обосновать выбор подходящего математического метода и привести алгоритм решения задачи; – анализировать приводимые представления конечных групп; **владеть:** – навыками построения и анализа моделей типичных операционных задач.			
8. Специализация **«Анализ безопасности информационных систем».** С целью получения данной специализации при изучении базовой части цикла обучающийся должен: **знать:** – математические основы моделирования распределенных систем (графовая модель, сети Петри, логические модели, потоковые модели), модели программ; – формальные методы и подходы к верификации программного обеспечения; – практические основы построения систем статического и динамического анализа программ; – методы анализа и тестирования протоколов; – основы теории формальной спецификации и верификации программного обеспечения; – способы защиты систем от исследования и отладки;	**7-10**	Верификация безопасности информационных систем Анализ безопасности протоколов Математический аппарат и средства анализа безопасности программного обеспечения	ПСК 8.1 ПСК 8.2 ПСК 8.3 ПСК 8.4

Продолжение цикла С.2				
	– подходы к испытанию средств криптографической защиты и требования к встраиванию криптосистем в информационные системы; – методы и алгоритмы дизассемблирования программ; – современные средства отладки и эмуляции программного кода; – методы восстановления алгоритма программы по ее дизассемблированному коду, а также методы построения графа передачи управления программы по исполняемому коду; **уметь:** – формализовать задачи анализа безопасности информационных систем, определять объем необходимых тестов и контрольных экспериментов, разрабатывать методики испытаний, применять существующие инструментальные средства статического и динамического анализа программного обеспечения, средства мониторинга и аудита безопасности; – разрабатывать модели нарушителя и угроз для информационных систем, выделять подсистемы и модули, содержащие критическую информацию; – создавать формальное описание протоколов с целью их дальнейшего анализа; – дизассемблировать и отлаживать программу; – выявить атаку в информационных журналах системы, описать природу атаки, ее признаки и методы обнаружения, оценивать систему с точки зрения проведения возможных атак на систему; **владеть:** – методами и инструментальными средствами анализа безопасности программного обеспечения; – методами и средствами поиска уязвимостей, анализа и верификации			

Продолжение цикла С.2			
протоколов; – современными методами обработки результатов экспериментов для оценки полноты и достоверности испытаний; – методами и инструментарием эмуляции и виртуализации для проведения испытаний сложных систем; – инструментальными и аппаратными средствами для проверки функционала испытуемых систем; – общими подходами к испытанию систем криптографической защиты (аутентификация, защита данных); – типовыми средствами анализа сетевых протоколов; – современными средствами отладки и тестирования программы; – современными средствами поиска уязвимостей.			
9. Специализация **«Создание автоматизированных систем в защищенном исполнении»**. С целью получения данной специализации при изучении базовой части цикла обучающийся должен: **знать:** – основы теории электрорадиоизмерений; – основы теории надежности; – основы расчета единичных и комплексных показателей надежности автоматизированных систем и их компонентов; **уметь:** – определять необходимые устройства для измерения параметров информативных сигналов от технических средств обработки информации; – выбирать и оценивать различные структуры систем с точки зрения надежности; **владеть:** – методами обработки результатов электрорадиоизмерений;	**7-10**	Метрология и электрорадио-измерения Основы теории надежности Основы радиотехники	ПСК-9.1 ПСК-9.2 ПСК-9.3 ПСК-9.6

Продолжение цикла С.2			
– методами проектирования систем по заданным требованиям надежности.			
10. Специализация **«Информационная безопасность автоматизированных систем на транспорте»**. С целью получения данной специализации при изучении базовой части цикла обучающийся должен: **знать:** – языки описания цифрового автомата с памятью и методы синтеза схем цифрового автомата произвольного назначения на элементах различного базиса и степени интеграции; – влияние способов кодирования на сложность структуры цифрового автомата, его быстродействие, устойчивость работы (исключение состязаний) и надежность работы; – методы синтеза цифрового автомата с программируемой логикой; – основные методы разработки алгоритмов и программ, структуры данных, используемые для представления типовых информационных объектов; – основные задачи анализа алгоритмов; – основные машинные алгоритмы и характеристики их сложности для типовых задач, часто встречающихся и ставших "классическими" в области информатики и программирования; **уметь:** – получать стандартные формы представления цифрового автомата с памятью по их описанию на начальных языках; – синтезировать логические схемы блоков операционного и управляющего автоматов с использованием методов синтеза цифрового автомата; – разрабатывать алгоритмы,	**7-10**	Теория автоматов Структуры и алгоритмы обработки данных	ПСК-10.1 ПСК-10.2 ПСК-10.3 ПСК-10.9 ПСК-10.10

Продолжение цикла С.2				
	используя общие схемы, методы и приемы построения алгоритмов, выбирая подходящие структуры данных для представления информационных объектов; – доказывать корректность составленного алгоритма и оценивать основные характеристики его сложности; – реализовывать алгоритмы и используемые структуры данных средствами языков программирования высокого уровня; – исследовать эффективность алгоритма и программы; **владеть:** – навыками разработки алгоритмов и программ, структур данных, используемых для представления типовых информационных объектов; – системным подходом при построении алгоритмов; – навыками реализации алгоритмов и используемых структур данных, средствами языков программирования высокого уровня.			
	Вариативная часть (знания, умения, навыки определяются ООП вуза)	**9-14**		
С.3	**Профессиональный цикл**	**140-150**		
	Базовая (общепрофессиональная) часть В результате изучения базовой части цикла обучающийся должен: **знать:** – основные информационные технологии, используемые в автоматизированных системах; – опасные и вредные факторы системы «человек – среда обитания»; – научные и организационные основы защиты окружающей среды и ликвидации последствий аварий, катастроф, стихийных бедствий; – общие принципы построения и использования современных языков программирования высокого уровня; – язык программирования высокого	**102-108**[3]	Безопасность жизнедеятельности Языки программирования Технологии и методы программирования Электроника и схемотехника Безопасность операционных систем Безопасность сетей	ОК-1 ОК-2 ОК-5 ОК-6 ОК-7 ОК-8 ОК-9 ОК-10 ПК-3 ПК-4 ПК-5 ПК-6 ПК-7 ПК-8 ПК-9 ПК-10 ПК-11 ПК-12 ПК-13

Продолжение цикла С.3			
уровня (объектно-ориентированное программирование); – возможности, классификацию и область применения макрообработки; – способы обработки исключительных ситуаций; – современные технологии и методы программирования; – показатели качества программного обеспечения; – методологии и методы проектирования программного обеспечения; – методы тестирования и отладки программного обеспечения; – принципы организации документирования разработки, процесса сопровождения программного обеспечения; – основные структуры данных и способы их реализации на языке программирования; – основные комбинаторные и теоретико-графовые алгоритмы, а также способы их эффективной реализации и оценки сложности; – основы теории электрических цепей; – принципы работы элементов и функциональных узлов электронной аппаратуры; – методы анализа и синтеза электронных схем; – типовые схемотехнические решения основных узлов и блоков электронной аппаратуры; – принципы построения и функционирования, примеры реализаций современных операционных систем; – функции операционных систем, основные концепции управления процессорами, памятью, вспомогательной памятью, устройствами; – критерии оценки эффективности и надежности средств защиты операционных систем; – принципы организации и структуру		ЭВМ Безопасность систем баз данных Основы информационной безопасности Криптографические методы защиты информации Организация ЭВМ и вычислительных систем Техническая защита информации Сети и системы передачи информации Организационное и правовое обеспечение информационной безопасности Программно-аппаратные средства обеспечения информационной безопасности Разработка и эксплуатация защищенных автоматизированных систем Управление информационной безопасностью	ПК-14 ПК-15 ПК-16 ПК-17 ПК-18 ПК-19 ПК-20 ПК-21 ПК-22 ПК-23 ПК-24 ПК-25 ПК-26 ПК-27 ПК-28 ПК-29 ПК-30 ПК-31 ПК-32 ПК-33 ПК-34 ПК-35 ПК-36 ПК-37 ПК-38 ПК-39 ПК-40

Продолжение цикла С.3				
	подсистем защиты операционных систем семейств UNIX и Windows; – принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей; – основные протоколы компьютерных сетей; – последовательность и содержание этапов построения компьютерных сетей; – эталонную модель взаимодействия открытых систем; – основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в компьютерных сетях; – принципы построения и функционирования, архитектуру, примеры реализаций современных систем управления базами данных; – основные модели данных, физическую организацию баз данных; – средства обеспечения безопасности данных; – последовательность и содержание этапов проектирования баз данных; – сущность и понятие информации, информационной безопасности и характеристику ее составляющих; – место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России; – источники и классификацию угроз информационной безопасности; – основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; – основные задачи и понятия криптографии; – требования к шифрам и основные характеристики шифров;		Инженерная графика	

Продолжение цикла С.3				
	– типовые поточные и блочные шифры; – частотные характеристики открытых текстов и способы их применения к анализу простейших шифров замены и перестановки; – типовые шифры с открытыми ключами; – модели шифров и математические методы их исследования; – архитектуру, принципы функционирования, элементную базу современных компьютеров, вычислительных и телекоммуникационных систем; – терминологию, основные руководящие и регламентирующие документы в области ЭВМ, комплексов и систем; – технические характеристики, показатели качества ЭВМ и систем, методы их оценки и пути совершенствования; – технические каналы утечки информации; – возможности технических средств перехвата информации; – способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; – организацию защиты информации от утечки по техническим каналам на объектах информатизации; – основы физической защиты объектов информатизации; – основные характеристики сигналов электросвязи, спектры и виды модуляции; – принципы построения и функционирования систем и сетей передачи информации; – способы кодирования информации; – основные телекоммуникационные протоколы; – основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые			

Продолжение цикла С.3				
	акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации; – правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны и служб защиты информации на предприятиях; – организацию 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; – программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, компьютерных сетях; – основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; – автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности; – методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем; – содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности			

Продолжение цикла С.3				
	автоматизированных систем; – методы, способы и средства обеспечения отказоустойчивости автоматизированных систем; – основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические); – основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения информационной безопасности в автоматизированных и телекоммуникационных системах; – основные методы управления информационной безопасностью; – методы аттестации уровня защищенности автоматизированных систем; – принципы формирования политики информационной безопасности в автоматизированных системах; – основные положения стандартов Единой системы конструкторской документации, Единой системы программной документации; **уметь:** – реализовывать и контролировать выполнение требований по охране труда и технике безопасности в профессиональной деятельности; – применять основные методы защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий; – работать с интегрированной средой разработки программного обеспечения; – использовать шаблоны классов и средства макрообработки; – использовать динамически подключаемые библиотеки; – формировать требования и разрабатывать внешние спецификации для разрабатываемого программного обеспечения; – планировать разработку сложного			

Продолжение цикла С.3				
	программного обеспечения; – проектировать структуру и архитектуру программного обеспечения с использованием современных методологий и средств автоматизации проектирования программного обеспечения; – проводить комплексное тестирование и отладку программных систем; – проектировать и кодировать алгоритмы с соблюдением требований к качественному стилю программирования; – реализовывать основные структуры данных и базовые алгоритмы средствами языков программирования; – проводить выбор эффективных способов реализации структур данных и конкретных алгоритмов при решении профессиональных задач; – применять на практике методы анализа электрических цепей; – работать с современной элементной базой электронной аппаратуры; – использовать стандартные методы и средства проектирования цифровых узлов и устройств, в том числе для средств защиты информации; – использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем; – оценивать эффективность и надежность защиты операционных систем; – планировать политику безопасности операционных систем; – проектировать и администрировать компьютерные сети, реализовывать политику безопасности компьютерной сети; – эффективно использовать различные методы и средства			

Продолжение цикла С.3			
защиты информации для компьютерных сетей; – проводить мониторинг угроз безопасности компьютерных сетей; – разрабатывать и администрировать базы данных и интерфейсы прикладных программ к базам данных; – реализовывать политику безопасности баз данных; – выделять сущности и связи предметной области; – отображать предметную область на конкретную модель данных; – нормализовывать отношения при проектировании реляционной базы данных; – создавать объекты базы данных; – выполнять запросы к базе данных; – разрабатывать прикладные программы, осуществляющие взаимодействие с базами данных; – применять средства обеспечения безопасности данных; – классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; – классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; – эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах; – применять математические методы исследования моделей шифров; – проводить анализ архитектуры и структуры ЭВМ и систем, оценивать эффективность архитектурно-технических решений, реализованных при построении ЭВМ и систем; – осуществлять сбор, обработку, анализ и систематизацию научно-технической информации в области ЭВМ и систем с применением современных информационных технологий;			

Продолжение цикла С.3				
	– анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем; – пользоваться нормативными документами по противодействию технической разведке; – анализировать и оценивать угрозы информационной безопасности объекта; – применять знания о системах электрической связи для решения задач по созданию защищенных телекоммуникационных систем; – анализировать тенденции развития систем и сетей электросвязи, внедрения новых служб и услуг связи; – применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; – разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации; – проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы; – разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем; – администрировать подсистемы информационной безопасности автоматизированных систем; – восстанавливать работоспособность подсистемы			

Продолжение цикла С.3				
	информационной безопасности автоматизированных систем в нештатных ситуациях; – исследовать эффективность создаваемых средств автоматизации, проводить технико-экономическое обоснование проектных решений; – разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов; – определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; – разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем; – выявлять уязвимости информационно-технологических ресурсов автоматизированных систем, проводить мониторинг угроз безопасности автоматизированных систем; – оценивать информационные риски в автоматизированных системах; – определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем; – составлять аналитические обзоры по вопросам обеспечения информационной безопасности автоматизированных систем; – разрабатывать частные политики информационной безопасности автоматизированных систем; – контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем; – разрабатывать предложения по			

Продолжение цикла С.3				
	совершенствованию системы управления информационной безопасностью автоматизированных систем; – применять требования Единой системы конструкторской документации и Единой системы программной документации при разработке технической документации; **владеть:** – профессиональной терминологией в области информационной безопасности; – навыками безопасного использования технических средств в профессиональной деятельности; – навыками проектирования программного обеспечения с использованием средств автоматизации; – навыками разработки, документирования, тестирования и отладки программного обеспечения в соответствии с современными технологиями и методами программирования; – навыками разработки программной документации; – навыками программирования с использованием эффективных реализаций структур данных и алгоритмов; – навыками использования измерительного оборудования при экспериментальном исследовании электронной аппаратуры; – навыками работы с программными средствами схемотехнического моделирования; – навыками чтения принципиальных схем, построения временных диаграмм и восстановления алгоритма работы узла, устройства и системы по комплекту документации; – навыками оценки быстродействия и оптимизации работы электронных схем на базе современной			

Продолжение цикла С.3				
	элементной базы; – навыками работы с современными операционными системами, восстановления операционных систем после сбоев; – навыками установки и настройки современных операционных систем с учетом требований по обеспечению информационной безопасности; – навыками эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности; – навыками разработки, документирования компьютерных сетей с учетом требований по обеспечению безопасности; – навыками использования программно-аппаратных средств обеспечения безопасности компьютерных сетей; – навыками разработки, документирования баз данных с учетом требований по обеспечению информационной безопасности; – криптографической терминологией; – навыками использования типовых криптографических алгоритмов; – навыками использования ЭВМ в анализе простейших шифров; – навыками математического моделирования в криптографии; – методиками оценки показателей качества и эффективности ЭВМ и вычислительных систем; – навыками работы с технической документацией на ЭВМ и вычислительные системы; – методами и средствами технической защиты информации; – методами расчета и инструментального контроля показателей технической защиты			

Продолжение цикла С.3				
	информации; – навыками анализа основных характеристик и возможностей телекоммуникационных систем по передаче информации; – навыками работы с нормативными правовыми актами; – навыками организации и обеспечения режима секретности; – методами организации и управления деятельностью служб защиты информации на предприятии; – методами формирования требований по защите информации; – навыками работы с технической документацией на компоненты автоматизированных систем на русском и иностранном языках; – навыками анализа основных узлов и устройств современных автоматизированных систем; – навыками поддержания работоспособности, обнаружения и устранения неисправностей в работе электронных аппаратных средств автоматизированных систем; – методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем; – навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем; – навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем; – навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности; – методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных			

Продолжение цикла С.3				
	систем; – методами управления информационной безопасностью автоматизированных систем; – методами оценки информационных рисков; – навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем; – навыками разработки технической документации в соответствии с требованиями Единой системы конструкторской документации и Единой системы программной документации.			
	1. Специализация **«Автоматизированные информационные системы специального назначения»**[2]	**9-11**		
	2. Специализация **«Высокопроизводительные вычислительные системы специального назначения»**[2]	**9-11**		
	3. Специализация **«Информационная безопасность автоматизированных систем критически важных объектов».** С целью получения данной специализации при изучении базовой части цикла обучающийся должен: **знать:** – характеристики основных технических каналов утечки информации на критически важных объектах; – методы и процедуры выявления угроз информационной безопасности на критически важных объектах; – средства защиты информации, используемые на критически важных объектах; – тактико-технические характеристики и возможности систем и средств технической разведки; – способы и средства охраны объектов;	**9-11**	Обеспечение информационной безопасности на критически важных объектах Инженерно-техническая защита информации и технические средства охраны на критически важных объектах Основы аттестации объектов информатизации критически важных объектов Методы и средства противодействия террористической	ПСК – 3.1 ПСК – 3.2 ПСК – 3.3 ПСК – 3.4 ПСК – 3.5 ПСК – 3.6

Продолжение цикла С.3			
уметь: – формулировать основные требования к методам и средствам технической защиты информации на критически важных объектах; – реализовывать с учетом особенностей функционирования критически важных объектов требования нормативно-методической и руководящей документации, а также действующего законодательства по вопросам защиты информации ограниченного доступа; – составлять и оформлять акты контрольных проверок, анализировать результаты проверок и разрабатывать предложения по совершенствованию и повышению эффективности применения мер по технической защите информации на критически важных объектах; **владеть:** – терминологией и системным подходом построения защищенных автоматизированных систем критически важных объектов; – навыками анализа угроз и уязвимостей информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов; – навыками формирования политик безопасности для критически важных объектов и автоматизированных систем критически важных объектов; – навыками проведения специальных исследований и инструментального контроля защищенности автоматизированных систем критически важных объектов; – навыками работы с нормативными правовыми актами в области технической защиты информации ограниченного доступа на предприятии (в организации, учреждении).		деятельности в системах управления критически важных объектов	
4. Специализация **«Безопасность открытых**	**9-11**	Информационная безопасность	ПСК-4.1 ПСК-4.2

Продолжение цикла С.3			
информационных систем». С целью получения данной специализации при изучении базовой части цикла обучающийся должен: **знать:** – подходы к интеграции сетей в открытых информационных системах; – принципы работы сетевых протоколов и технологий передачи данных в открытых информационных системах; – основные методы и средства реализации удаленных сетевых атак на открытые информационные системы; – о политиках безопасности и мерах защиты в открытых информационных системах; – о комплексном подходе к построению эшелонированной защиты для открытых информационных систем; – принципы построения современных виртуальных локальных и частных сетей и направления их развития; – виды виртуальных сетей и их преимущества при конкретном применении; – политику безопасности для виртуальных сетей; – основные стандарты построения виртуальных сетей; – принципы работы сетевых протоколов и технологий передачи данных в виртуальных сетях; – подходы к интеграции виртуальных сетей с открытыми информационными системами; **уметь:** – проектировать защищенные открытые информационные системы; – определять и устранять основные угрозы информационной безопасности для открытых информационных систем; – строить модель нарушителя информационной безопасности для		открытых систем Виртуальные частные сети Аудит информационных технологий и систем обеспечения информационной безопасности	ПСК-4.3 ПСК-4.4 ПСК-4.5 ПСК-4.6 ПСК-4.7 ПСК-4.8

Продолжение цикла С.3				
	открытых информационных систем; – выявлять и устранять уязвимости в основных компонентах открытых информационных систем; – обнаруживать, прерывать и предотвращать удаленные сетевые атаки по их характерным признакам; – применять стандартные решения для защиты информации в открытых информационных системах и квалифицированно оценивать их качество; – используя современные методы и средства, разрабатывать и оценивать модели и политику безопасности для открытых информационных систем; – реализовывать системы защиты информации в открытых информационных системах в соответствии со стандартами по оценке защищенных систем; – практически решать задачи защиты программ и данных программно-аппаратными средствами и давать оценку качества предлагаемых решений; – осуществлять мониторинг и аудит сетевой безопасности; – осуществлять администрирование открытых информационных систем; – осуществлять управление информационной безопасностью в открытых информационных системах; – применять стандартные решения для защиты информации в виртуальных сетях и квалифицированно оценивать их качество; – используя современные методы и средства, разрабатывать и оценивать модели и политику безопасности для виртуальных сетей; – практически реализовывать различные варианты построения виртуальных сетей в соответствии со стандартами по оценке защищенных систем и давать оценку качества предлагаемых решений;			

Продолжение цикла С.3			
– проектировать защищенные открытые информационные системы; **владеть:** – терминологией и системным подходом построения защищенных открытых информационных систем и виртуальных сетей; – навыками анализа угроз информационной безопасности и уязвимостей в открытых информационных системах; – навыками анализа угроз и навыками построения политик безопасности для открытых информационных систем и виртуальных сетей.			
5. Специализация **«Информационная безопасность автоматизированных банковских систем»**. С целью получения данной специализации при изучении базовой части цикла обучающийся должен: **знать:** – основные методы защиты информации в автоматизированных банковских системах; – о комплексном подходе к построению эшелонированной защиты для автоматизированных банковских систем; – методы электронного документооборота в автоматизированных банковских системах; – основные методы обеспечения безопасности пластиковых карт; **уметь:** – проводить синтез и анализ проектных решений по обеспечению информационной безопасности автоматизированных банковских систем; – эффективно применять информационно-технологические ресурсы автоматизированных банковских систем с учетом требований информационной безопасности;	**9-11**	Защита информации в банковских системах Защита электронного документооборота Безопасность систем пластиковых карт Нормативная база обеспечения информационной безопасности банковской организации	ПСК - 5.1 ПСК - 5.2 ПСК - 5.3 ПСК - 5.4 ПСК - 5.5 ПСК - 5.6 ПСК - 5.7 ПСК - 5.8 ПСК - 5.9 ПСК - 5.10

Продолжение цикла С.3				
	– разрабатывать и реализовывать политики информационной безопасности автоматизированных банковских систем; – проектировать и эксплуатировать системы управления информационной безопасностью автоматизированных банковских систем; – проводить инструментальный мониторинг защищенности автоматизированных банковских систем; – разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных банковских систем; – формировать и эффективно применять комплекс мер (правил, процедур, практических приемов, руководящих принципов, методов, средств) для обеспечения информационной безопасности автоматизированных банковских систем; **владеть:** – терминологией и системным подходом построения защищенных автоматизированных банковских систем; – навыками анализа угроз информационной безопасности и уязвимостей в автоматизированных банковских системах; – навыками анализа угроз и формирования политик безопасности для автоматизированных банковских систем; – навыками формирования и эффективного применения комплекса мер (правил, процедур, практических приемов, руководящих принципов, методов, средств) для обеспечения информационной безопасности автоматизированных банковских систем и банковских организаций.			

Продолжение цикла С.3			
6. Специализация **«Защищенные автоматизированные системы управления»** С целью получения данной специализации при изучении базовой части цикла обучающийся должен: **знать:** – принципы защиты программного обеспечения защищенных автоматизированных систем управления от несанкционированного копирования с привязкой к магнитным носителям, регистрационным кодам и специальным аппаратным устройствам защиты (электронным ключам); – средства защиты программного обеспечения защищенных автоматизированных систем управления; – современные системы проектирования программного и аппаратного обеспечения защищенных автоматизированных систем управления; – основы построения систем менеджмента информационной безопасности на базе современных международных и национальных стандартов; – основные критерии, методы и меры обеспечения доверия к информационной безопасности; **уметь:** – применять инструментальные средства для исследования программного обеспечения защищенных автоматизированных систем управления в машинных кодах; – выявлять уязвимости защиты программного обеспечения защищенных автоматизированных систем управления и находить пути их устранения; – проектировать и реализовывать защиту программного обеспечения	**9-11**	Защита программного обеспечения защищенных автоматизированных систем Технологии проектирования защищенных автоматизированных систем Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления Обеспечение доверия к информационной безопасности защищенных автоматизированных систем управления	ПСК - 6.1 ПСК - 6.2 ПСК - 6.3 ПСК - 6.4 ПСК - 6.5 ПСК - 6.6 ПСК - 6.7

Продолжение цикла С.3				
	защищенных автоматизированных систем управления, исходя из поставленных целей защиты; – разрабатывать модели жизненного цикла защищенных автоматизированных систем управления с учетом требований по обеспечению информационной безопасности на основе современных международных и национальных стандартов; – применять основные положения системного и объектно-ориентированного проектирования и моделирования защищенных автоматизированных систем управления; – разрабатывать, реализовывать, оценивать и корректировать основные процессы управления информационной безопасностью; – выбирать, разрабатывать и внедрять практические меры по управлению информационной безопасностью на основе современных международных и национальных стандартов; **владеть:** – навыками работы с современными инструментальными средствами для исследования программного обеспечения защищенных автоматизированных систем управления; – навыками разработки защиты программного обеспечения для защищенных автоматизированных систем управления; – навыками автоматизации и управления процессом проектирования защищенных автоматизированных систем управления; – навыками разработки систем мониторинга информационной безопасности защищенных автоматизированных систем управления; – навыками применения различных			

Продолжение цикла С.3			
методов и мер обеспечения доверия к информационной безопасности: лицензирование, аккредитация, оценка и подтверждение соответствия.			
7. Специализация **«Обеспечение информационной безопасности распределенных информационных систем».** С целью получения данной специализации при изучении базовой части цикла обучающийся должен: **знать:** – основные положения теории управления; – специфику математического моделирования организационных задач в автоматизированных системах; – способы обеспечения информационной безопасности систем организационного управления; – принципы построения распределенных систем и объектно-ориентированных систем управления базами данных, технологии автоматизированного проектирования баз данных и хранилищ данных, требования к архитектуре информационных систем и их компонентам для обеспечения безопасности функционирования; – нормативные документы по метрологии, стандартизации и сертификации программных и аппаратных средств защиты; **уметь:** – разрабатывать модели систем организационного управления; – использовать технологии автоматизированного проектирования и структурный подход при проектировании информационных систем, определять ресурсы, необходимые для обеспечения безопасности информационной системы, использовать методы и средства определения технологической безопасности	**9-11**	Информационная безопасность распределенных информационных систем Методы проектирования защищенных распределенных информационных систем Технология построения защищенных распределенных приложений	ПСК-7.1 ПСК-7.2 ПСК-7.3 ПСК-7.4 ПСК-7.5 ПСК-7.6 ПСК-7.7 ПСК-7.8 ПСК-7.9

Продолжение цикла С.3				
	функционирования распределенной информационной системы; – применять нормативные документы по метрологии, стандартизации и сертификации на практике; **владеть:** – навыками разработки политики безопасности систем организационного управления; – навыками семантического моделирования данных, навыками проектирования информационных систем на базе корпоративных систем управления базами данных, методами снижения угроз безопасности информационных систем, вызванных ошибками на этапе проектирования, разработки и внедрения; – навыками разработки документации по метрологии, стандартизации и сертификации программных и аппаратных средств защиты.			
	8. Специализация **«Анализ безопасности информационных систем»** С целью получения данной специализации при изучении базовой части цикла обучающийся должен: **знать:** – принципы построения современных систем обеспечения информационной безопасности; – принципы статистического анализа; – способы описания поведения систем; – типовые архитектуры и принципы построения современных защищенных информационных систем; – угрозы и атаки, характерные для распределенных информационных систем; **уметь:** – формализовать задачу контроля параметров безопасности	**9-11**	Мониторинг безопасности информационных систем Анализ рисков информационной безопасности	ПСК – 8.2 ПСК – 8.3 ПСК – 8.5 ПСК – 8.6

Продолжение цикла С.3			
информационными системами; – разрабатывать методы и средства для проверки выполнения требований информационной безопасности и поиска уязвимостей; **владеть:** – методиками оценки рисков информационной безопасности; – средствами фиксации параметров безопасности информационных систем; – методами реализации и верификации моделей контроля и управления доступом; – навыками применения средств анализа безопасности информационных систем.			
9. Специализация **«Создание автоматизированных систем в защищенном исполнении»** С целью получения данной специализации при изучении базовой части цикла обучающийся должен: **знать:** – методы и процедуры выявления угроз и нарушителей информационной безопасности процессов создания и эксплуатации автоматизированных систем в защищенном исполнении; – методы и средства для обеспечения информационной безопасности автоматизированных систем в защищенном исполнении на различных стадиях и этапах их жизненного цикла; – современные технологии проектирования автоматизированных систем в защищенном исполнении; – нормативную правовую базу, руководящие и методические документы, регламентирующие реализацию процессов создания автоматизированных систем в защищенном исполнении на различных стадиях их жизненного цикла; – методы и средства анализа	**9-11**	Угрозы информационной безопасности автоматизированных систем Создание автоматизированных систем в защищенном исполнении Оценка информационной безопасности автоматизированных систем в защищенном исполнении	ПСК-9.1 ПСК-9.2 ПСК-9.3 ПСК-9.4 ПСК-9.5 ПСК-9.6

Продолжение цикла С.3			
достаточности мер по обеспечению информационной безопасности процессов создания и эксплуатации автоматизированных систем в защищенном исполнении; **уметь:** – разрабатывать модели угроз и нарушителей информационной безопасности процессов создания и эксплуатации автоматизированных систем в защищенном исполнении; – формировать требования по обеспечению информационной безопасности автоматизированных систем в защищенном исполнении; – разрабатывать проектные решения по автоматизированным системам в защищенном исполнении, их системам обеспечения информационной безопасности, реализовывать их, управлять процессами разработки и реализации этих проектных решений; – проводить анализ достаточности мер по обеспечению информационной безопасности процессов создания и эксплуатации автоматизированных систем в защищенном исполнении; **владеть:** – терминологией и технологиями проектирования автоматизированных систем в защищенном исполнении; – навыками анализа достаточности мер по обеспечению информационной безопасности процессов создания и эксплуатации автоматизированных систем в защищенном исполнении; – навыками проведения специальных исследований и инструментального контроля защищенности автоматизированных систем в защищенном исполнении.			
10. Специализация **«Информационная безопасность автоматизированных систем на транспорте»**	**9-11**	Информационная безопасность информационно-управляющих и	ПСК-10.1 ПСК-10.2 ПСК-10.3 ПСК-10.4

Продолжение цикла С.3			
С целью получения данной специализации при изучении базовой части цикла обучающийся должен: **знать:** – основы комплексного обеспечения информационной безопасности распределенных автоматизированных, информационно-управляющих и информационно-логистических систем транспорта; – основные свойства схем шифрования, электронной цифровой подписи и аутентификации при решении задач защиты технологического электронного документооборота и документоведения; – принципы применения и построения систем управления ресурсами предприятия и технологий поддержки жизненного цикла, методы и средства обеспечения их информационной безопасности; **уметь:** – используя современные методы и средства, разрабатывать и оценивать модели и политики безопасности автоматизированных и информационно-управляющих систем на транспорте; – анализировать, оценивать и исключать уязвимости информационной безопасности в автоматизированных и информационно-управляющих системах на транспорте, применять автоматизированные средства мониторинга, аудита и анализа защищенности данных систем; – реализовывать системы защиты информации в распределенных автоматизированных, информационно-управляющих и информационно-логистических системах на транспорте в соответствии со стандартами по		информационно-логистических систем транспорта Защита информации в распределенных информационных системах и центрах обработки данных Информационная безопасность автоматизированных транспортных систем Защита электронного технологического документооборота	ПСК-10.5 ПСК-10.6 ПСК-10.7 ПСК-10.8 ПСК-10.9 ПСК-10.10

Продолжение цикла С.3				
	оценке защищенных систем; – обеспечивать защиту электронного технологического документооборота на основе электронной цифровой подписи; – решать практические задачи информационной безопасности на основе инфраструктуры открытых ключей; – обеспечивать безопасность систем управления ресурсами предприятия и технологий поддержки жизненного цикла; **владеть:** – навыками анализа угроз и уязвимостей информационной безопасности в автоматизированных и информационно-управляющих системах на транспорте; – навыками анализа угроз и навыками построения политик безопасности распределенных автоматизированных информационно-управляющих и информационно-логистических систем транспорта; – навыками развертывания и обеспечения работы программных комплексов, обеспечивающих работу с цифровыми сертификатами; – методами эксплуатации средств защиты информации; – системным подходом к организации информационных процессов (в том числе систем управления ресурсами предприятия и технологий поддержки жизненного цикла), анализу информационной безопасности распределенных автоматизированных информационно-управляющих и информационно-логистических систем транспорта.			
	Вариативная часть (знания, умения, навыки определяются ООП вуза)	**38-42**		
С.4	**Физическая культура**	**2**		ОК-11 ОК-12

С.5	**Учебная и производственная практики, научно-исследовательская работа** (практические умения и навыки определяются ООП вуза)	**15-18**		ОК-1 – ОК-11 ПК-1 – ПК-40 ПСК-1.1 – ПСК-10.10
С.6	**Итоговая государственная аттестация**	**18-21**		ОК-3 ОК-5 ОК-7 – ОК-10 ПК-1 – ПК-22 ПК-29 ПК-31 – ПК-34 ПСК-1.1 – ПСК-10.10
	Общая трудоемкость основной образовательной программы	**300**		

[1] Трудоемкость циклов С.1, С.2, С.3 и разделов С.4, С.5 включает все виды текущей и промежуточной аттестаций.

[2] В соответствии с п. 7.1 настоящего стандарта требования к результатам освоения и структуре ООП в части специализаций определяются вузом.

[3] Суммарная трудоемкость базовых составляющих циклов С.1, С.2 и С.3 должна составлять не менее 75 процентов от общей трудоемкости указанных циклов.

VII. ТРЕБОВАНИЯ К УСЛОВИЯМ РЕАЛИЗАЦИИ ОСНОВНЫХ ОБРАЗОВАТЕЛЬНЫХ ПРОГРАММ ПОДГОТОВКИ СПЕЦИАЛИСТА

7.1. Образовательные учреждения самостоятельно разрабатывают и утверждают ООП подготовки специалиста, которая включает в себя учебный план, рабочие программы учебных курсов, предметов, дисциплин (модулей) и другие материалы, обеспечивающие воспитание и качество подготовки обучающихся, а также программы учебной и производственной практик, календарный учебный график и методические материалы, обеспечивающие реализацию соответствующей образовательной технологии.

Специализация ООП подготовки специалиста определяется высшим учебным заведением в соответствии с ФГОС ВПО и примерной ООП подготовки специалиста.

Требования к результатам освоения и структуре ООП подготовки специалистов в части специализаций для вузов, в которых предусмотрена военная служба и (или) служба в правоохранительных органах, определяются вузами по согласованию с федеральными органами исполнительной власти, в ведении которых находятся данные образовательные учреждения.

Реализация ООП по специальности **090303 Информационная безопасность автоматизированных систем** допускается только при наличии у вуза лицензии на проведение работ, связанных с использованием сведений, составляющих государственную тайну.

В случае если ООП связана с освоением учебного материала, содержащего сведения, составляющие государственную тайну, то условия ее реализации должны соответствовать следующим требованиям:

наличие у лиц, участвующих в реализации образовательного процесса, содержащего сведения, составляющие государственную тайну, оформленного в установленном порядке допуска к государственной тайне по соответствующей форме;

наличие в образовательном учреждении нормативных правовых актов по обеспечению режима секретности и их выполнение;

осуществление образовательного процесса, содержащего сведения, составляющие государственную тайну, только в помещениях образовательного учреждения либо организаций, на базе которых реализуется образовательный процесс, удовлетворяющих требованиям нормативных правовых актов по режиму секретности, противодействию техническим разведкам и технической защите информации;

использование при реализации образовательного процесса, содержащего сведения, составляющие государственную тайну, средств вычислительной техники и программного обеспечения, удовлетворяющих требованиям нормативных правовых актов по режиму секретности,

противодействию техническим разведкам и технической защите информации.

Высшие учебные заведения обязаны ежегодно обновлять ООП подготовки специалиста с учетом развития науки, техники, культуры, экономики, технологий и социальной сферы.

7.2. При разработке ООП подготовки специалиста должны быть определены возможности вуза в формировании общекультурных компетенций выпускников (компетенций социального взаимодействия, самоорганизации и самоуправления, системно-деятельностного характера). Вуз обязан сформировать социокультурную среду, создать условия, необходимые для всестороннего развития личности.

Вуз обязан способствовать развитию социально-воспитательного компонента учебного процесса, включая развитие студенческого самоуправления, участие обучающихся в работе общественных организаций, спортивных и творческих клубов, научных студенческих обществ.

7.3. Реализация компетентностного подхода должна предусматривать широкое использование в учебном процессе активных и интерактивных форм проведения занятий (компьютерных симуляций, деловых и ролевых игр, разборов конкретных ситуаций, психологических и иных тренингов) в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся. В рамках учебных курсов, связанных с проблемами обеспечения информационной безопасности, должны быть предусмотрены встречи с представителями органов государственной власти и управления, российских компаний, государственных и общественных организаций, мастер-классы экспертов и специалистов.

Удельный вес занятий, проводимых в интерактивных формах, определяется главной целью ООП подготовки специалиста, особенностью контингента обучающихся и содержанием конкретных дисциплин. В целом,

в учебном процессе они должны составлять не менее 25 процентов аудиторных занятий, в том числе специальных профессиональных деловых игр (комплексных учений) в объеме не менее одной недели. Занятия лекционного типа для соответствующих групп обучающихся не могут составлять более 55 процентов аудиторных занятий.

7.4. В учебной программе каждой дисциплины (модуля) должны быть четко сформулированы конечные результаты обучения в органичной увязке с осваиваемыми знаниями, умениями и приобретаемыми компетенциями в целом по ООП подготовки специалиста.

Общая трудоемкость дисциплины не может быть менее двух зачетных единиц (за исключением дисциплин по выбору обучающихся и факультативных дисциплин). По дисциплинам, трудоемкость которых составляет более трех зачетных единиц, должна выставляться оценка («отлично», «хорошо», «удовлетворительно» , «неудовлетворительно»).

7.5. ООП подготовки специалиста должна содержать дисциплины по выбору обучающихся в объеме не менее одной трети вариативной части суммарно по циклам С.1, С.2 и С.3. Порядок формирования дисциплин по выбору обучающихся устанавливает ученый совет вуза.

7.6. Максимальный объем учебной нагрузки обучающихся не может составлять более 54 академических часов в неделю, включая все виды аудиторной и внеаудиторной (самостоятельной) учебной работы по освоению ООП и факультативных дисциплин, устанавливаемых вузом дополнительно к ООП подготовки специалиста и необязательных для изучения обучающимися.

Объем факультативных дисциплин не должен превышать 13 зачетных единиц за весь период обучения.

7.7. Объем аудиторных учебных занятий в неделю при освоении ООП в очной форме обучения составляет не менее 27 и не более 36 академических

часов. В указанный объем не входят обязательные аудиторные занятия по физической культуре.

7.8. В случае реализации ООП подготовки специалиста в иных формах обучения максимальный объем аудиторных занятий устанавливается в соответствии с Типовым положением об образовательном учреждении высшего профессионального образования (высшем учебном заведении), утвержденным постановлением Правительства Российской Федерации № 71 от 14 февраля 2008 г. (Собрание законодательства Российской Федерации, 2008, № 8, ст. 731).

7.9. Обший объем каникулярного времени в учебном году должен составлять 7-10 недель, в том числе не менее двух недель в зимний период.

В высших учебных заведениях, в которых предусмотрена военная служба и (или) служба в правоохранительных органах, продолжительность каникулярного времени обучающихся определяется в соответствии с нормативными правовыми актами, регламентирующими порядок прохождения службы*.

7.10. Раздел «Физическая культура» («Физическая подготовка» - для вузов, в которых предусмотрена военная служба и (или) служба в правоохранительных органах) трудоемкостью две зачетные единицы реализуется: при очной форме обучения, как правило, в объеме 400 часов, при этом объем практической, в том числе игровых видов, подготовки должен составлять не менее 360 часов.

7.11. Вуз обязан обеспечить обучающимся реальную возможность участвовать в формировании своей программы обучения, включая возможную разработку индивидуальных образовательных программ.

7.12. Вуз обязан ознакомить обучающихся с их правами и обязанностями при формировании ООП подготовки специалиста, разъяснить,

---

* Статья 30 Положения о порядке прохождения военной службы, утвержденного Указом Президента Российской Федерации от 16 сентября 1999 г. № 1237 «Вопросы прохождения военной службы» (Собрание законодательства Российской Федерации, 1999, № 38, ст. 4534).

что избранные обучающимися дисциплины (модули) становятся для них обязательными.

7.13. ООП подготовки специалиста вуза должна включать лабораторные практикумы и практические занятия по дисциплинам (модулям) базовой части циклов С.2 и С.3, формирующим у обучающихся умения и навыки в области физики, электроники и схемотехники, сетей и систем передачи информации, технологии и методов программирования, безопасности сетей ЭВМ, безопасности операционных систем, безопасности систем баз данных, программно-аппаратных средств обеспечения информационной безопасности, технической защиты информации, а также по дисциплинам специализации и вариативной части, рабочие программы которых предусматривают цели формирования у обучающихся соответствующих умений и навыков.

7.14. Наряду с установленными законодательными и другими нормативными правовыми актами, правами и обязанностями обучающиеся имеют следующие права и обязанности:

обучающиеся имеют право в пределах объема учебного времени, отведенного на освоение дисциплин (модулей) по выбору, предусмотренных ООП подготовки специалиста, выбирать конкретные дисциплины (модули);

при формировании своей индивидуальной образовательной программы обучающиеся имеют право получить консультацию в вузе по выбору дисциплин (модулей) и их влиянию на будущую специализацию ООП подготовки специалиста;

обучающиеся при переводе из другого высшего учебного заведения при наличии соответствующих документов имеют право на перезачет освоенных ранее дисциплин (модулей) на основании аттестации;

обучающиеся обязаны выполнять в установленные сроки все задания, предусмотренные ООП подготовки специалиста.

7.15. Раздел ООП подготовки специалиста «Учебная и

производственная практики, научно-исследовательская работа» является обязательным и представляет собой форму организации учебного процесса, непосредственно ориентированную на профессионально-практическую подготовку обучающихся.

Конкретные виды практик определяются ООП вуза. Цели и задачи, программы и формы отчетности определяются вузом по каждому виду практики.

Практики проводятся в сторонних организациях, основная деятельность которых предопределяет наличие объектов и видов профессиональной деятельности выпускников по данной специальности (специализации) или на кафедрах и в лабораториях вуза (учебная практика), обладающих необходимым кадровым и научно-техническим потенциалом.

В высших учебных заведениях, в которых предусмотрена военная служба и (или) служба в правоохранительных органах, за счет времени, выделяемого на практики, могут проводиться специальные профессиональные деловые игры (комплексные учения).

Аттестация по итогам практики проводится на основании оформленного в соответствии с установленными требованиями письменного отчета и отзыва руководителя практики от организации. По итогам аттестации выставляется оценка («отлично», «хорошо», «удовлетворительно», «неудовлетворительно»).

7.16. Научно-исследовательская работа является обязательным разделом ООП подготовки специалиста. Она направлена на комплексное формирование общекультурных, профессиональных и профессионально-специализированных компетенций в соответствии с требованиями ФГОС ВПО.

При разработке программы научно-исследовательской работы высшее учебное заведение должно предоставить возможность обучающимся:

изучать специальную литературу и другую научно-техническую информацию о достижениях отечественной и зарубежной науки и техники в соответствующей области знаний;

участвовать в проведении научных исследований или выполнении технических разработок;

осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме (заданию);

принимать участие в стендовых и промышленных испытаниях опытных образцов (партий) проектируемых изделий;

составлять отчеты (разделы отчета) по теме или ее разделу (этапу, заданию), готовить рефераты;

выступать с докладом на конференции, научном семинаре.

В процессе выполнения научно-исследовательской работы и оценки ее результатов должно проводиться широкое обсуждение в учебных структурах вуза с привлечением работодателей, позволяющее оценить уровень компетенций, сформированных у обучающегося. Необходимо также дать оценку компетенций, связанных с формированием профессионального мировоззрения и определения уровня культуры.

7.17. Реализация ООП подготовки специалиста должна обеспечиваться научно-педагогическими кадрами, имеющими, как правило, базовое образование, соответствующее профилю преподаваемой дисциплины, и систематически занимающимися научной и (или) научно-методической деятельностью.

Доля преподавателей, имеющих ученую степень и (или) ученое звание, в общем числе преподавателей, обеспечивающих образовательный процесс по данной ООП, должна быть не менее 65 процентов, ученую степень доктора наук (в том числе степень, присваиваемую за рубежом, документы о присвоении которой прошли установленную процедуру признания и

установления эквивалентности) и (или) ученое звание профессора должны иметь не менее 9 процентов преподавателей.

Преподаватели профессионального цикла должны иметь базовое образование и (или) ученую степень, соответствующие профилю преподаваемой дисциплины, или опыт деятельности в сфере обеспечения информационной безопасности.

Не менее 70 процентов преподавателей (в приведенных к целочисленным значениям ставок), обеспечивающих учебный процесс по профессиональному циклу, должны иметь ученые степени или ученые звания, при этом ученые степени доктора наук или ученое звание профессора должны иметь не менее 11 процентов преподавателей.

К образовательному процессу должно быть привлечено не менее пяти процентов преподавателей из числа действующих руководителей и работников профильных организаций, предприятий и учреждений.

До 10 процентов от общего числа преподавателей, имеющих ученую степень и (или) ученое звание может быть заменено преподавателями, имеющими стаж практической работы по данному направлению на должностях руководителей или ведущих специалистов не менее 5 последних лет.

В вузах, в которых предусмотрена военная служба и (или) служба в правоохранительных органах, к преподавателям с учеными степенями и (или) учеными званиями приравниваются преподаватели военно-(специальных) профессиональных дисциплин, не имеющие ученых степеней и ученых званий, имеющие профильное высшее образование, опыт работы в войсках (на флотах), штабах, правоохранительных органах, учреждениях не менее 10 лет, воинское звание не ниже «подполковник», а также или боевой опыт, или государственные награды, или государственные (отраслевые) почетные звания, или государственные премии. В числе преподавателей с ученой степенью доктора наук и (или) ученым званием профессора могут учитываться преподаватели военно-(специальных) профессиональных учебных

дисциплин с ученой степенью кандидата наук, имеющие или государственные награды, или государственные (отраслевые) почетные звания, или государственные премии.

В структуре вуза, реализующего данную ООП подготовки специалиста, должна быть отдельная выпускающая кафедра по специальности «Информационная безопасность автоматизированных систем».

Общее руководство содержанием теоретической и практической подготовки по специализации должно осуществляться штатным научно-педагогическим работником вуза, имеющим ученую степень доктора или кандидата наук и (или) ученое звание профессора или доцента, стаж работы в образовательных учреждениях высшего профессионального образования не менее трех лет. К общему руководству содержанием теоретической и практической подготовки по специализации может быть привлечен высококвалифицированный специалист в соответствующей сфере профессиональной деятельности.

7.18. ООП подготовки специалиста должна обеспечиваться учебно-методической документацией и материалами по всем учебным курсам, дисциплинам (модулям) ООП. Содержание каждой из таких учебных дисциплин (модулей) должно быть представлено в сети Интернет или локальной сети образовательного учреждения с выполнением установленных требований по защите информации.

Внеаудиторная работа обучающихся должна сопровождаться методическим обеспечением и обоснованием времени, затрачиваемого на ее выполнение.

Каждый обучающийся должен быть обеспечен доступом к электронно-библиотечной системе, содержащей издания по основным изучаемым дисциплинам и сформированной на основании прямых договоров с правообладателями учебной и учебно-методической литературы.

При этом должна быть обеспечена возможность осуществления одновременного индивидуального доступа к такой системе не менее чем для 25 процентов обучающихся.

Библиотечный фонд должен быть укомплектован печатными и (или) электронными изданиями основной учебной литературы по дисциплинам базовой части всех циклов, изданными за последние 10 лет (для дисциплин базовой части гуманитарного, социального и экономического цикла – за последние пять лет), из расчета не менее 25 экземпляров таких изданий на каждые 100 обучающихся.

Фонд дополнительной литературы помимо учебной должен включать официальные, справочно-библиографические и специализированные периодические издания, в том числе нормативные правовые акты и нормативные методические документы в области информационной безопасности, в расчете один-два экземпляра на каждые 100 обучающихся.

Электронно-библиотечная система должна обеспечивать возможность индивидуального доступа для каждого обучающегося из любой точки, в которой имеется доступ к сети Интернет, с выполнением установленных требований по защите информации.

Оперативный обмен информацией с отечественными и зарубежными вузами и организациями должен осуществляться с соблюдением требований законодательства Российской Федерации об интеллектуальной собственности и защиты сведений, составляющих государственную тайну, а также международных договоров Российской Федерации в области интеллектуальной собственности. Для обучающихся должен быть обеспечен доступ к современным профессиональным базам данных, информационным справочным и поисковым системам, в том числе по тематике информационной безопасности.

Каждому обучающемуся должен быть обеспечен доступ к комплектам библиотечного фонда, состоящего не менее чем из пяти наименований отечественных и не менее четырех наименований зарубежных журналов.

7.19. Ученый совет высшего учебного заведения при введении ООП подготовки специалиста утверждает размер средств на реализацию соответствующих ООП.

Финансирование реализации ООП подготовки специалиста должно осуществляться в объеме не ниже установленных нормативов финансирования высшего учебного заведения*.

7.20. Высшее учебное заведение, реализующее ООП подготовки специалистов, должно располагать материально-технической базой, включая приборы, оборудование и программно-аппаратные средства специального назначения, обеспечивающей проведение всех видов дисциплинарной и междисциплинарной подготовки, лабораторной, практической и научно-исследовательской работы обучающихся, предусмотренных учебным планом вуза и соответствующей действующим санитарным и противопожарным правилам и нормам.

Минимально необходимый для реализации ООП подготовки специалистов перечень материально-технического обеспечения включает в себя:

лаборатории в области:

- физики;
- электроники и схемотехники;
- сетей и систем передачи информации;
- технической защиты информации;
- программно-аппаратных средств обеспечения информационной безопасности;

---

* Пункт 2 статьи 41 Закона Российской Федерации «Об образовании» от 10 июля 1992 г. № 3266 -1 (Собрание законодательства Российской Федерации, 1996, № 3, ст. 150; 2002, № 26, ст. 2517; 2004, № 30, ст. 3086; № 35, ст. 3607; 2005, № 1, ст. 25; 2007, № 17, ст. 1932; № 44, ст. 5280).

- технологии и методов программирования;
- безопасности сетей ЭВМ.

Лаборатории высшего учебного заведения должны быть оснащены современным оборудованием, стендами, приборами, позволяющими изучать и исследовать аппаратуру и процессы в соответствии с реализуемой ООП.

Специально оборудованные кабинеты и аудитории в области:

- иностранного языка;
- информатики;
- Интернет - технологий;
- сетевых компьютерных технологий;
- безопасности операционных систем;
- безопасности систем баз данных.

Лаборатории и специально оборудованные кабинеты и аудитории должны быть предусмотрены также для реализации дисциплин (модулей) специализации и вариативной части, рабочие программы которых предусматривают цели формирования у обучающихся соответствующих умений и навыков.

Компьютерные классы должны быть оборудованы современной вычислительной техникой для занятий по дисциплинам из расчета одно рабочее место на одного обучаемого при проведении занятий в данных классах.

При использовании электронных изданий и проведении самостоятельной подготовки вуз должен обеспечить обучающихся возможностью выхода в сеть Интернет из расчета не менее одного рабочего места на 10 обучающихся по данной ООП.

Вуз должен быть обеспечен необходимым комплектом лицензионного программного обеспечения и сертифицированными программными и аппаратными средствами защиты информации.

VIII. ТРЕБОВАНИЯ К ОЦЕНКЕ КАЧЕСТВА ОСВОЕНИЯ ОСНОВНЫХ ОБРАЗОВАТЕЛЬНЫХ ПРОГРАММ ПОДГОТОВКИ СПЕЦИАЛИСТА

8.1. Высшее учебное заведение обязано обеспечивать гарантию качества подготовки, в том числе путем:

разработки стратегии по обеспечению качества подготовки выпускников с привлечением представителей работодателей;

мониторинга, периодического рецензирования образовательных программ;

разработки объективных процедур оценки уровня знаний и умений обучающихся, компетенций выпускников;

обеспечения компетентности преподавательского состава;

регулярного проведения самообследования по согласованным критериям для оценки деятельности (стратегии) и сопоставления с другими образовательными учреждениями с привлечением представителей работодателей;

информирования общественности о результатах своей деятельности, планах, инновациях.

8.2. Оценка качества освоения ООП подготовки специалиста должна включать текущий контроль успеваемости, промежуточную аттестацию обучающихся и итоговую государственную аттестацию выпускников.

8.3. Конкретные формы и процедуры текущего и промежуточного контроля знаний по каждой дисциплине разрабатываются вузом самостоятельно и доводятся до сведения обучающихся в течение первого месяца от начала обучения по соответствующей дисциплине.

8.4. Для аттестации обучающихся на соответствие их персональных достижений поэтапным требованиям соответствующей ООП подготовки специалиста (текущий контроль успеваемости и промежуточная аттестация) создаются фонды оценочных средств, включающие типовые задания,

контрольные работы, тесты и методы контроля, позволяющие оценить знания, умения и уровень сформированности компетенций. Фонды оценочных средств разрабатываются и утверждаются вузом.

Фонды оценочных средств должны быть полными и адекватными отображениями требований ФГОС ВПО по данному направлению подготовки (специальности), соответствовать целям и задачам конкретной ООП подготовки специалиста и её учебному плану. Они призваны обеспечивать оценку качества общекультурных, профессиональных и профессионально-специализированных компетенций, приобретаемых выпускником в соответствии с этими требованиями.

При разработке оценочных средств для контроля качества изучения модулей, дисциплин, практик должны учитываться все виды связей между включенными в них знаниями, умениями, навыками, позволяющие установить качество сформированных у обучающихся компетенций и степень общей готовности выпускников к профессиональной деятельности.

Вузом должны быть созданы условия для максимального приближения системы контроля качества освоения обучающимися ООП к условиям их будущей профессиональной деятельности. С этой целью, кроме преподавателей конкретной дисциплины, в качестве внешних экспертов должны активно привлекаться работодатели (представители заинтересованных организаций), преподаватели, читающие смежные дисциплины.

8.5. Обучающимся должна быть предоставлена возможность оценивания содержания, организации и качества учебного процесса в целом, а также работы отдельных преподавателей.

8.6. Итоговая государственная аттестация направлена на установление соответствия уровня профессиональной подготовки выпускников требованиям ФГОС ВПО.

Итоговая государственная аттестация включает защиту выпускной квалификационной работы (дипломного проекта, дипломной работы). Государственный экзамен вводится по решению ученого совета вуза.

Требования к содержанию, объему и структуре выпускной квалификационной работы, а также требования к государственному экзамену (при наличии) определяются вузом.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Квалификация	Срок обуч.
специалист	5

ФГБОУ ВПО "ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ"
ФГБОУ ВПО "ДГТУ"

Утверждаю

Ректор / Т.А. ИСМАИЛОВ /

"02" 07 2012 г.

План одобрен Ученым советом вуза
30.06.2011 протокол № 11

Шифр плана в ИМЦА

РАБОЧИЙ УЧЕБНЫЙ ПЛАН

специалистов очная форма обучения

090303 - "Информационная безопасность автоматизированных систем"

090303 65

специализация "Безопасность открытых информационных систем"

График учебного процесса

Курс	Сентябрь 1-7 сен	8-14 сен	15-21 сен	22-28 сен	29 сен - 5 окт	Октябрь 6-12 окт	13-19 окт	20-26 окт	27 окт - 02 ноя	Ноябрь 3-9 ноя	10-16 ноя	17-23 ноя	24 ноя - 30 ноя	Декабрь 1-7 дек	8-14 дек	15-21 дек	22-28 дек	29 дек - 4 янв	Январь 5-11 янв	12-18 янв	19-25 янв	26 янв - 1 фев	Февраль 2-8 фев	9-15 фев	16-22 фев	23 фев - 1 мар
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=
1																			Э	Э	Э	К	К			
2																			Э	Э	Э	К	К			
3																			Э	Э	Э	К	К			
4																			Э	Э	Э	К	К			
5																				Э	Э	Э	К	К	Г	Г

Курс	Март 2-8 мар	9-15 мар	16-22 мар	23-29 мар	30 мар - 5 апр	Апрель 6-12 апр	13-19 апр	20-26 апр	27 апр - 3 май	Май 4-10 май	11-17 май	18-24 май	25-31 май	Июнь 1-7 июн	8-14 июн	15-21 июн	22-28 июн	29 июн - 5 июл	Июль 6-12 июл	13-19 июл	20-26 июл	27 июл - 2 авг	Август 3-9 авг	10-16 авг	17-23 авг	24-30 авг
	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52
	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=
1																Э	Э	Э	К	К	К	К	К	К	К	К
2																Э	Э	Э	У	У	К	К	К	К	К	К
3																Э	Э	Э	П	П	К	К	К	К	К	К
4																Э	Э	Э	П	П	К	К	К	К	К	К
5	П	П	П	П	П	П	Д	Д	Д	Д	Д	Д	Д	Д	Д	Д	Д	Д	К	К	К	К	К	К	К	К

Курс	Недель: Теоретическое обучение О	В	Итого	Экзаменационные сессии	Итоговая Аттестация	Учебная практика	Другие Практики, НИР	Дипломная работа (ВКР)	Гос. Экзамены и защита	Каникулы	Всего	Студентов	Групп
1	18	18	36	6						10	52		
2	18	18	36	6		2				8	52		
3	18	18	36	6			2			8	52		
4	18	18	36	6			2			8	52		
5	19		19	3			6	12	2	10	52		
			153	27		2	10	12	2	44	260		

Обозначения:
- [ ] - Теоретическое обучение
- [Э] - Экзаменационные сессии
- [У] - Учебная практика
- [П] - Другие Практики, НИР
- число - Наличие распределенной практики или НИР
- [ ] - Переаттестовано
- [Д] - Дипломная работа (ВКР)
- [Г] - Гос. Экзамены и защита
- [К] - Каникулы
- [А] - Итоговая Аттестация
- [=] - Неделя отсутствует

Распределение по курсам и семестрам

№	Название дисциплины	Экзамены	Зачеты	Курсовые проекты	Курсовые работы	Всего, ч	Всего по ГОС	Аудиторные	КСР	Сам. работа	1 сем.	2 сем.	3 сем.	4 сем.	5 сем.	6 сем.	7 сем.	8 сем.	9 сем.	Закрепленная кафедра	Итого ЗЕТ	Всего ЗЕТ по плану	Перечень компетенций	[illegible]	[illegible]
(32 35)	С1 Гуманитарный, социальный и экономический цикл										Всего ЗЕТ 35+29+10											29			29
С1.Б.1	Философия	5				144	144	72		36					36 36					55	4	4		14	4
С1.Б.2	История Отечества	1				144	144	72		36	36 36									17	4	4		14	4
С1.Б.3	Иностранный язык	4	123			396	396	198		162	54	54	36	54						13	11	11		40	11
С1.Б.4	Правоведение		6			108	108	54		54						36 18				34	3	3		12	3
С1.Б.5	Экономика	3				144	144	72		36			36 36							61	4	4		14	4
С1.Б.6	Основы управленческой деятельности		9			108	108	38		70									19 19	24	3	3		10	3
С1.В	Русский язык и культура речи		1			108	108	54		54	54									42	3	3		12	3
С1.В.2	Гуманитарные аспекты информационной безопасности	7				144	144	72		36							36 36			36	4	4		4	4
Б (24 29)	В (8 10)	5	6			1296	1295	632		434	36 144	54	36 72	54	36 36	36 18	36 36		19 19		36	36		30	36
	С1.ДВ1 Дисциплины по выбору																					3			
1	Политология		8			108	108	54		54								36 18		34	3	3		12	3
2	Социология		8			108	108	54		54								36 18		55	3	3		12	
	Всего по циклу	5	7			1404	1404	686		538	36 144	54	36 72	54	36 36	36 18	36 36	36 18	19 19		39	39		142	39
(74 85)	С2 Математический и естественнонаучный цикл										Всего ЗЕТ 75+65+10											65			65
С2.Б.1	Алгебра и геометрия	12				324	324	162		72	36 36	36 54								7	9	5		34	5
С2.Б.2	Математический анализ	12				432	432	216		126	54 54	54 54								7	12	12		42	12
С2.Б.3	Дискретная математика	4	3			288	288	144		108			18 36	36 18 36						36	8	8		28	8
С2.Б.4	Теория вероятностей и математическая статистика	3	4			216	216	108		72			36 18	18 18 18						8	6	6		22	6
С2.Б.5	Математическая логика и теория алгоритмов	6	5			180	180	90		54					18 18	5 18 18				36	5	5		20	5
С2.Б.6	Теория информации		5			108	108	54		54					36 18					36	3	3		12	3
С2.Б.7	Информатика		1			108	108	54		54	36 18									15	3	3		12	3
С2.Б.8	Физика	2	12			432	432	216		180	36 18 18	54 18 36	18 18							53	12	12		42	12
С2.Б.9	Открытые информационные системы		6			108	108	54		54						36 18				36	3	3		12	3
С2.Б.10	Криптографические протоколы и стандарты	7				144	144	72		36							36 36			36	4	4		16	4
С2.В.1	Дифференциальные уравнения		2			108	108	54		54		36 18								7	3	3		12	3
С2.В.2	Случайные процессы		7			108	108	54		54							36 18			36	3	3		12	3
Б (63 69)	В (9 14)	9	10			2556	2556	1278		918	162 36 108	180 18 162	72 72	54 36 54	54 36	54 36 18	72 36 18				71	71		264	71
	С2.ДВ1 Дисциплины по выбору																					4			
1	Интегрированные программные средства	7				144	144	72		36							36 36			36	4	4		16	4
2	Основы визуального программирования	7				144	144	72		36							36 36			8	4	4		16	
	Всего по циклу	10	10			2700	2700	1350		954	162 36 108	180 18 162	72 72	54 36 54	54 36	54 36 18	108 72 18				75	75		280	75
(140 150)	С3 Профессиональный цикл										Всего ЗЕТ 145=104+4											104			104
С3.Б.1	Безопасность жизнедеятельности		7			72	72	36		36							18 18			11	2	2		3	2
С3.Б.2	Языки программирования	3	2			288	288	144		108		18 36 18	36 18 18							36	8	8		30	8
С3.Б.3	Технологии и методы программирования	4				216	216	108		72			18 18	36 36						36	6	6		22	6
С3.Б.4	Электроника и схемотехника	5	4			288	288	144		108				18 36	54 36					63	8	8		30	8
С3.Б.5	Безопасность операционных систем	5	4			288	288	144		108				36 36	36 36					36	8	8		30	8
С3.Б.6	Безопасность сетей ЭВМ	6	5			360	360	162		162					36 36	54 36				36	10	10		34	10
С3.Б.7	Безопасность систем баз данных	7	6			288	288	144		108						18 18	54 54			36	8	8		30	8
С3.Б.8	Основы информационной безопасности	2				144	144	72		36		36 36								36	4	4		14	4
С3.Б.9	Криптографические методы защиты информации	8				144	144	72		36								36 36		35	4	4		14	4
С3.Б.10	Организация ЭВМ и вычислительных систем	5	7			288	288	144		108						54 36	18 36			3	8	8		28	8
С3.Б.11	Техническая защита информации	8				144	144	72		36								36 36		36	4	4		14	4
С3.Б.12	Сети и системы передачи информации	6	5			180	180	90		54					18 18	36 18				36	5	5		18	5
С3.Б.13	Организационное и правовое обеспечение информационной безопасности		9			108	108	57		51									38 19	26	3	3		12	3
С3.Б.14	Программно-аппаратные средства обеспечения ИБ	8				180	180	90		54								54 36		36	5	5		18	5
С3.Б.15	Разработка и эксплуатация защищенных АС	8				180	180	90		54								54 36		37	5	5		[illegible]	5
С3.Б.16	Управление информационной безопасностью	9				180	180	95		49									57 38	36	5	5		[illegible]	[illegible]
С3.Б.17	Инженерная графика		1			72	72	36		36	18 18										2	2		[illegible]	[illegible]
С3.Б.18	Информационная безопасность открытых систем		7			108	108	54		54							36 18			36	3	3		[illegible]	[illegible]
С3.Б.19	Виртуальные частные сети		8			108	108	54		54								36 18		26	3	3		[illegible]	[illegible]

Распределение по курсам и семестрам

№	Название дисциплины	Экзамены	Зачеты	Курсовые проекты	Курсовые работы	Всего с ЗЕ	Всего по ГОС	Аудиторные	КСР	Самостоятельная работа
Б.5.20	Аудит информационных технологий и систем обеспечения ИБ		9			108	108	57		51
С3.В.1	Операционные системы	4				180	180	90		54
С3.В.2	Системы управления базами данных	5				144	144	72		36
С3.В.3	Теоретические основы компьютерной безопасности		6			108	108	54		54
С3.В.4	Защита программ и данных	9				144	144	76		32
С3.В.5	Комплексное обеспечение ИБ автоматизированных систем		8			108	108	54		54
С3.В.6	Методы программирования	3				144	144	72		36
С3.В.7	Документоведение		1			108	108	54		54
Б.1(02.108)	Б.158.42	18	17			4680	4680	2337		1695
	С3.ДВ1 Дисциплины по выбору									
1	Обеспечение ИБ в банковской системе	9				180	180	76		68
2	Обеспечение ИБ в интеллектуальных системах	9				180	180	76		68
	С3.ДВ2 Дисциплины по выбору									
1	Методы оценки безопасности компьютерных систем	9				144	144	76		32
2	Информационно-аналитические работы по обеспечению ИБ АС	9				144	144	76		32
	С3.ДВ3 Дисциплины по выбору									
1	Организация работы администратора АС		9			108	108	57		51
2	Катастрофоустойчивость информационных систем		9			108	108	57		51
	С3.ДВ4 Дисциплины по выбору									
1	Информационные технологии		3			108	108	54		54
2	Защита электронного документооборота		3			108	108	54		54
	Всего	20	19			5220	5220	2600		1900
	Всего									
	Всего									
7	С4	Физическая культура								
С4.Б.1	Физическая культура		[illegible]			400	400	400		
	Всего		8			400	400	400		
	Итого	35	44			9724	9724	5036		3392

№	1 сем. Лекции	Лаб.	Практ.	КСР	2 сем. Лекции	Лаб.	Практ.	КСР	3 сем. Лекции	Лаб.	Практ.	КСР	4 сем. Лекции	Лаб.	Практ.	КСР	5 сем. Лекции	Лаб.	Практ.	КСР
Б.5.20																				
С3.В.1													36	54						
С3.В.2																	36	36		
С3.В.3																				
С3.В.4																				
С3.В.5																				
С3.В.6									36	36										
С3.В.7	18		36																	
Б.1(02.108)	36		54		54	36	54		90	72	18		126	152			180	162		
ДВ1 1																				
ДВ1 2																				
ДВ2 1																				
ДВ2 2																				
ДВ3 1																				
ДВ3 2																				
ДВ4 1									36	18										
ДВ4 2									36	18										
Всего	36		54		54	36	54		126	90	18		126	162			180	162		
Всего																				
Всего																				
С4									Всего ЗЕТ 2											
С4.Б.1			40				32				46				52				54	
Всего			40				32				46				52				54	
Итого	234	36	346		234	54	302		234	162	136		180	198	170		270	198	90	

№	6 сем. Лекции	Лаб.	Практ.	КСР	7 сем. Лекции	Лаб.	Практ.	КСР	8 сем. Лекции	Лаб.	Практ.	КСР	9 сем. Лекции	Лаб.	Практ.	КСР	ЗЕ	Всего ЗЕТ	Всего ЗЕТ по плану	Примечание	[illegible]	[illegible]
Б.5.20													38	19			36	3	3		14	3
С3.В.1																	36	5	5		18	5
С3.В.2																	36	4	4		14	4
С3.В.3	36	18															36	3	3		12	3
С3.В.4													38	38			36	4	4		16	4
С3.В.5									36	18							36	3	3		12	3
С3.В.6																	36	4	4		14	4
С3.В.7																	24	3	3		12	3
Б.1(02.108)	158	126			126	126			252	80			171	114				150	150		484	150
																			15			
ДВ1 1													38	38			36	5	5		14	5
ДВ1 2													38	38			36	5	5		14	
ДВ2 1													38	38			36	4	4		14	4
ДВ2 2													38	38			36	4	4		14	
ДВ3 1													38	19			36	3	3		12	3
ДВ3 2													38	19			36	3	3		12	
ДВ4 1																	36	3	3		12	3
ДВ4 2																	36	3	2		12	
Всего	198	126			126	126			252	180			285	209				145	145		536	145
Всего																						
Всего																						
С4																			2			2
С4.Б.1			58				54				54							2	2			2
Всего			58				54				54							2	2			2
Итого	288	162	94		270	198	108		288	180	72		304	209	19			261	261		958	261
																					26,7%	

	Итого	1 сем.	2 сем.	3 сем.	4 сем.	5 сем.	6 сем.	7 сем.	8 сем.	9 сем.
Обязательных уч. часов в неделю / физ-ра / физ-ры		32 / 2	31 / 2	27 / 3	27 / 3	28 / 3	27 3	29 / 3	27 / 2	28 /
Обязательных экзаменов	35	3 Нед 2	4 Нед 3	4 Нед 2	4 Нед 3	4 Нед 3	4 Нед 2	4 Нед 1	4 Нед 3	4 Нед 2
Обязательных зачетов	36	6	3	5	3	4	4	4	3	4
Обязательных курсовых проектов, к. р.										
Обязательных курсовых работ										

Начальник ОМО УП Л.М. Меджидова

Проректор-начальник УМУ ____________ / К.А. Гасанов /

Начальник УО ____________ / Р.А. Атаханов /

Декан ____________ / А.Г. Мустафаев /

Зав. кафедрой ____________ / Э.Э. Ильясов /

Начальник ОМО УП ____________ / Л.М. Меджидова /

ФГБОУ ВПО "ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ"

ФГБОУ ВПО "ДГТУ"

Рабочий учебный план: 090303 - "Информационная безопасность автоматизированных систем" специализация "Безопасность открытых информационных систем"

Утвержден: Ректор _____ / Т.А. ИСМАИЛОВ / "___"_____ 2012 г. 090303.04_65-11-12345-3072.pli

Курс	Теоретическое обучение: Итого АЧ					ЗЕТ	Cr ECTS	Спец. виды работ: Итоговая аттестация (А)				Практики (У,П), НИР (П)				Дипломная работа (проект) (Д)				Гос. экзамены (ИГА) (Г)				АЧ	ЗЕТ	Cr ECTS
	Ауд	СРС	Изуч	Экз	Всего			Нед	АЧ	ЗЕТ	Cr ECTS	Нед	АЧ	ЗЕТ	Cr ECTS	Нед	АЧ	ЗЕТ	Cr ECTS	Нед	АЧ	ЗЕТ	Cr ECTS			
1	1 206	738	1 944	288	2 232	60	55,5																	2 232	60	55,5
2	1 080	792	1 872	288	2 160	57	60					2	108	3	3									2 268	60	63
3	1 102	738	1 840	288	2 128	57	59					2	108	3	3									2 236	60	62
4	1 116	720	1 836	288	2 124	57	59					2	108	3	3									2 232	60	62
5	532	404	936	144	1 080	30	30					6	324	9	9	12	648	18	17,75	2	108	3	3	2 160	60	59,75
6																										
7																										
Всего:	5036	3392	8428	1296	9724	261	263,5					12	648	18	18	12	648	18	17,75	2	108	3	3	11128	300	302,25

Распределение зачетных единиц по циклам

Часть Учебный цикл (раздел)	1 С1			2 С2			3 С3			4 Физкультура			5 Практики, НИР			6 ИГА			Факультативы		Всего		
	min	max	План	min	max	План	min	max	План	min	max	План	min	max	План	min	max	План	max	План	min	max	План
Базовая	24	29	29	65	69	65	102	108	104												191	206	198
Вариативная	8	10	10	9	14	10	38	42	41												55	66	61
Итого	32	39	39	74	83	75	140	150	145	2	2	2	15	18	18	18	21	21		-	281	313	300
Точность вычисления ЗЕТ	0,50	Точность вычисления ЗЕТ (А,У,П,Д,Г)					0,25			Д --> ИГА						Без факультативов					281	313	300
Подлежит изучению ЗЕТ																							300

Доля базовых дисциплин в общем объеме дисциплин по первым трем циклам (в ЗЕТ)	76,4%
Доля дисциплин по выбору студента в общем объеме вариативной части по первым трем циклам (в ЗЕТ)	36,1%
Доля лекционных занятий (в ЧАС)	49,7%
Доля зачятий в интерактивной форме (в ЧАС)	20,7%

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФГБОУ ВПО "ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ"
ФГБОУ ВПО "ДГТУ"

Квалификация	Срок обуч. (по ФГОС)
специалист	5

Утверждаю
Ректор _____ / М.Д. ИСМАИЛОВ /
"02" 02 2012 г.

План одобрен Ученым советом вуза
30.06.2011 протокол № 11

Шифр плана в ИМЦА

РАБОЧИЙ УЧЕБНЫЙ ПЛАН

090303 | 65

специалистов очная форма обучения
090303 - "Информационная безопасность автоматизированных систем"

специализация "Безопасность открытых информационных систем"

График учебного процесса

К У Р С	Сентябрь					Октябрь				Ноябрь				Декабрь					Январь				Февраль				Март					Апрель				Май				Июнь				Июль				Август				Недель								Студентов	Групп	К У Р С
	1-7 сен	8-14 сен	15-21 сен	22-28 сен	29 сен - 5 окт	6-12 окт	13-19 окт	20-26 окт	27 окт - 02 ноя	3-9 ноя	10-16 ноя	17-23 ноя	24 ноя - 30 ноя	1-7 дек	8-14 дек	15-21 дек	22-28 дек	29 дек - 4 янв	5-11 янв	12-18 янв	19-25 янв	26 янв - 1 фев	2-8 фев	9-15 фев	16-22 фев	23 фев - 1 мар	2-8 мар	9-15 мар	16-22 мар	23-29 мар	30 мар - 5 апр	6-12 апр	13-19 апр	20-26 апр	27 апр - 3 май	4-10 май	11-17 май	18-24 май	25-31 май	1-7 июн	8-14 июн	15-21 июн	22-28 июн	29 июн - 5 июл	6-12 июл	13-19 июл	20-26 июл	27 июл -2 авг	3-9 авг	10-16 авг	17-23 авг	24-30 авг	Теоретическое обучение			Экзаменационные сессии	Итоговая Аттестация	Учебная практика	Другие Практики, НИР	Дипломная работа (ВКР)	Гос. Экзамены и защита	Каникулы	Всего			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	О	В	Итого										
1																			Э	Э	Э	К	К																		Э	Э	Э	К	К	К	К	К	К	К	К	18	18	36	6					10	52			1
2																			Э	Э	Э	К	К																		Э	Э	Э	У	У	К	К	К	К	К	К	18	18	36	6		2			8	52			2
3																			Э	Э	Э	К	К																		Э	Э	Э	П	П	К	К	К	К	К	К	18	18	36	6			2		8	52			3
4																			Э	Э	Э	К	К																		Э	Э	Э	П	П	К	К	К	К	К	К	18	18	36	6			2		8	52			4
5																				Э	Э	Э	К	К	Г	Г	П	П	П	П	П	П	Д	Д	Д	Д	Д	Д	Д	Д	Д	Д	Д	К	К	К	К	К	К	К	К	19		19	3			6	12	2	10	52			5
																																																				163	27		2	10	12	2	44	260			

Обозначения: - Теоретическое обучение; Э - Экзаменационные сессии; У - Учебная практика; П - Другие Практики, НИР; число - Наличие распределенной практики или НИР; Д - Дипломная работа (ВКР); Г - Гос. Экзамены и защита; К - Каникулы; А - Итоговая Аттестация; = - Неделя отсутствует; - Переаттестовано

Программа учебной практики

Цели и задачи

Основной целью практики является закрепление теоретических знаний и практических навыков работы с объектами информатизации, программным обеспечением автоматизированных рабочих мест, приобретение студентами практических навыков и компетенций в сфере профессиональной деятельности.

Задачами практики являются:

- изучение организационной структуры объектов информатизации и систем управления;

- ознакомление с содержанием основных работ и исследований, связанных с обеспечением информационной безопасности автоматизированных систем.

Реализуемые компетенции

ОК-1 ОК-2 ОК-6 ОК-7 ОК-9 ОК-11 ПК-1 ПК-2 ПК-5 ПК-6 ПК-9 ПК-10 ПК-17 ПК-26 ПК-27

Трудоемкость, з.е. 2

Результаты освоения дисциплины (модуля)

знать:

- содержание основных исследований, проводимых на объектах информатизации для обеспечения информационной безопасности.

уметь:

- использовать полученные знания в профессиональной деятельности, проводить исследования объектов информатизации на предмет определения уровня обеспечения информационной безопасности.

владеть:

- навыками работы с организационно-распорядительными документами предприятия в области информационной безопасности.

Программа производственной практики

Цели и задачи

Целью и задачей производственной практики является: закрепление и углубление теоретических знаний, полученных студентами при изучении дисциплин общепрофессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем информационной безопасности автоматизированных систем; формирования общего представления об информационной безопасности автоматизированных систем, методов и средств ее обеспечения; изучение источников информации и системы оценок эффективности применяемых мер обеспечения информационной безопасности. Место проведения практики: профильные организации, учреждения и предприятия, а в качестве исключения –кафедры и научные подразделения вуза.

Реализуемые компетенции

ОК-1 ОК-2 ОК-6 ОК-7 ОК-10 ПК-1 ПК-2 ПК-4 ПК-5 ПК-6 ПК-8 ПК-9 ПК-10 ПК-12 ПК-14 ПК-15 ПК-16 ПК-17 ПК-18 ПК-19 ПК-21 ПК-22 ПК-23 ПК-24 ПК-25 ПК-26 ПК-27 ПК-29 ПК-30 ПК-31 ПК-32 ПК-37 ПК-39

Трудоемкость, з.е. 4

Результаты освоения дисциплины (модуля)

знать:

- обязанности должностных лиц предприятия, обеспечивающих решение проблем информационной безопасности автоматизированных систем.

уметь:

- оценивать эффективность применяемых мер обеспечения информационной безопасности предприятия, разрабатывать нормативно-техническую документацию.

владеть:

- навыками проектирования систем обеспечения информационной безопасности, обслуживания программно-аппаратных комплексов, установленных на предприятии.

Программа производственной (преддипломной) практики

Цели и задачи

Целью и задачей производственной (преддипломной) практики является: подготовить студента к решению задач комплексного обеспечения информационной безопасности предприятия и к выполнению выпускной квалификационной работы. Место проведения практики: профильные предприятия, научно-исследовательские организации и учреждения, обладающие кадровым и научно-техническим потенциалом, необходимым для подготовки студентом выпускной квалификационной работы.

Реализуемые компетенции

ОК-1 ОК-2 ОК-6 ОК-7 ОК-10 ПК-1 ПК-2 ПК-4 ПК-5 ПК-6 ПК-8 ПК-9 ПК-10 ПК-11 ПК-12 ПК-14 ПК-15 ПК-16 ПК-17 ПК-18 ПК-19 ПК-20 ПК-21 ПК-22 ПК-23 ПК-24 ПК-25 ПК-26 ПК-29 ПК-30 ПК-32 ПК-34 ПК-37 ПК-39

Трудоемкость, з.е. 6

Результаты освоения дисциплины (модуля)

знать:

- задачи комплексного обеспечения информационной безопасности автоматизированных систем предприятия.

уметь:

- анализировать имеющуюся научно-техническую и производственную рекомендацию, осуществлять сбор и анализ исходных данных для выполнения выпускной квалификационной работы.

владеть:

- навыками работы с документацией в области обеспечения информационной безопасности предприятия, сбора и анализа данных для оценки уровня информационной безопасности предприятия.

Приложение 5. Аннотации к рабочим программам дисциплин

Аннотация рабочей программы учебной дисциплины «Философия»

1. Цели и задачи дисциплины: формирование представления о специфике философии как способе познания и духовного освоения мира, основных разделах современного философского знания, философских проблемах и методах их исследования; овладение базовыми принципами и приемами философского познания; введение в круг философских проблем, связанных с областью будущей профессиональной деятельности, выработка навыков работы с оригинальными и адаптированными философскими текстами.

Изучение дисциплины направлено на развитие навыков критического восприятия и оценки источников информации, умения логично формулировать, излагать и аргументированно отстаивать собственное видение проблем и способов их разрешения; овладение приемами ведения дискуссии, полемики, диалога.

2. Место дисциплины в структуре ООП:

дисциплина цикла ГСЭ;

специальные требования к входным знаниям, умениям и компетенциям студента не предусматриваются;

является предшествующей для специальных философских дисциплин (напр., "философия науки", философия техники"), если таковые предусмотрены учебным планом.

3. Требования к результатам освоения дисциплины:

Процесс изучения дисциплины направлен на формирование следующих компетенций:

способностью осуществлять свою деятельность в различных сферах общественной жизни с учетом принятых в обществе морально-нравственных и правовых норм, соблюдать принципы профессиональной этики (ОК-2);

способностью анализировать социально значимые явления и процессы, в том числе политического и экономического характера, мировоззренческие и философские проблемы, применять основные положения и методы гуманитарных, социальных и экономических наук при решении социальных и профессиональных задач (ОК-3);

способностью понимать движущие силы и закономерности исторического процесса, роль личности в истории, политической организации общества, способностью уважительно и бережно относиться к историческому наследию, толерантно воспринимать социальные и культурные различия (ОК-4);

способностью логически верно, аргументировано и ясно строить устную и письменную речь на русском языке, готовить и редактировать тексты профессионального назначения, публично представлять собственные и известные научные результаты, вести дискуссии (ОК-7);

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

способностью самостоятельно применять методы и средства познания, обучения и самоконтроля для приобретения новых знаний и умений, в том числе в новых областях, непосредственно не связанных со сферой профессиональной деятельности, развития социальных и профессиональных компетенций, к изменению вида своей профессиональной деятельности (ОК-10);

способностью понимать сущность и значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска и обработки больших объемов информации по профилю деятельности в глобальных ком-

пьютерных системах, сетях, в библиотечных фондах и в иных источниках информации (ПК-4);

способностью применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ПК-5);

способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере своей профессиональной деятельности (ПК-9);

способностью применять современные методы исследования с использованием компьютерных технологий (ПК-10).

В результате изучения дисциплины студент должен:

Знать: основные разделы и направления философии, методы и приемы философского анализа проблем.

Уметь: анализировать мировоззренческие, социально и личностно значимые философские проблемы, проводить исторический анализ событий, анализировать и оценивать социальную информацию; планировать и осуществлять свою деятельность с учетом результатов этого анализа.

Владеть: навыками публичной речи, аргументации, ведения дискуссии и полемики, практического анализа логики различного рода рассуждений; навыками критического восприятия информации; навыками письменного аргументированного изложения собственной точки зрения.

4. Содержание дисциплины

№ п/п	Наименование раздела дисциплины
1.	Философия, ее предмет и место в культуре
2.	Исторические типы философии. Философские традиции и современные дискуссии.
3.	Философская онтология
4	Теория познания
5	Философия и методология науки
6	Философская антропология
7	Социальная философия и философия истории

Аннотация рабочей программы учебной дисциплины «История»

1. Цели и задачи дисциплины:

Формирование у слушателей современного исторического мышления, понимания процессов развития всемирной и отечественной истории, места, роли и особенностей складывания и развития российского общества и государства, изучение исторического опыта обеспечения национальной безопасности России;

- изучение истории способствует формированию высокой гражданственности и политической культуры слушателей, воспитанию патриотизма и гуманизма, чувства ответственности за судьбу страны и укрепление ее достойного места в мировом сообществе;

- изучение истории направлено на развитие навыков критического восприятия и оценки источников информации, умения логично формулировать, излагать и аргументировано отстаивать собственное видение проблем и способов их разрешения, овладение приемами ведения дискуссии, полемики, диалога.

2. Место дисциплины в структуре ООП:

- дисциплина цикла ГСЭ;

- специальные требования к входным знаниям, умениям и компетенциям студента не предусматриваются;

3. Требования к результатам освоения основных образовательных программ бакалавриата:

Выпускник должен обладать следующими общекультурными компетенциями (ОК):

способностью действовать в соответствии с Конституцией Российской Федерации, исполнять свой гражданский и профессиональный долг, руководствуясь принципами законности и патриотизма (ОК-1);

способностью осуществлять свою деятельность в различных сферах общественной жизни с учетом принятых в обществе морально-нравственных и правовых норм, соблюдать принципы профессиональной этики (ОК-2);

способностью анализировать социально значимые явления и процессы, в том числе политического и экономического характера, мировоззренческие и философские проблемы, применять основные положения и методы гуманитарных, социальных и экономических наук при решении социальных и профессиональных задач (ОК-3);

способностью понимать движущие силы и закономерности исторического процесса, роль личности в истории, политической организации общества, способностью уважительно и бережно относиться к историческому наследию, толерантно воспринимать социальные и культурные различия (ОК-4);

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

способностью понимать сущность и значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска и обработки больших объемов информации по профилю деятельности в глобальных компьютерных системах, сетях, в библиотечных фондах и в иных источниках информации (ПК-4).

В результате изучения базовой части цикла студент должен

Знать:

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

- ключевые события истории России и мире с древности до наших дней, выдающихся деятелей отечественной истории;

- различные оценки и периодизации Отечественной истории.

Уметь:

- соотносить общие исторические процессы и отдельные факты; выявлять существенные черты исторических процессов, явлений и событий;

- извлекать уроки из исторических событий и на их основе принимать осознанные решения.

- осуществлять эффективный поиск информации и критику источников;

- получать, обрабатывать и сохранять источники информации;

- формулировать и аргументировано отстаивать собственную позицию по различным проблемам истории;

Владеть:

- представлениями о событиях российской и всемирной истории, основанными на принципе историзма;

- навыками анализа исторических источников;

- приемами ведения дискуссии и полемики.

4. Содержание дисциплины

№ п/п	Наименование раздела дисциплины
1.	История как наука
2.	У истоков отечественной истории. Зарождение и развитие древнерусской государственности.
3.	Основные тенденции и особенности развития российского централизованного государства (XV-XVII вв.).
4	Российская империя: вехи истории. (XVIII – конец XIX вв.)
5	Россия и мир в конце XIX – начале XX веков: от реформаторства к революции.
6	Советский период отечественной истории (1917-1991 г.)
7	Основные тенденции развития современной России в конце XX – начале XXI вв.

Аннотация рабочей программы учебной дисциплины «Правоведение»

1. Цели и задачи дисциплины:

- приобретение слушателями необходимых государственно-правовых знаний;
- формирование правового сознания и правовой культуры студентов;
- развитие юридического мышления и формирование способности ориентироваться в государственно-правовых явлениях.

2. Место дисциплины в структуре ООП:

Дисциплина «Правоведение» входит в гуманитарный, социальный и экономический цикл.

3. Требования к результатам освоения дисциплины:

2.5. Процесс изучения дисциплины направлен на формирование следующих компетенций:

- способности осознавать необходимость соблюдения Конституции Российской Федерации, прав и обязанностей гражданина своей страны, гражданского долга и проявления патриотизма (ОК-1);
- способности осуществлять свою деятельность в различных сферах общественной жизни с учётом принятых в обществе моральных и правовых норм (ОК-2);
- способности 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 профессиональных задач (ОК-3);
- способности находить организационно-управленческие решения в нестандартных ситуациях и нести за них ответственность (ОК-6);
- способности 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);
- способности использовать нормативные правовые документы в своей профессиональной деятельности (ПК-3);
- способности формировать комплекс мер по информационной безопасности с учётом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности (ПК-4);

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

- способности организовывать 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).

В результате изучения дисциплины студент должен:

Знать:

- основы: российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации;

- характеристику основных отраслей российского права;

- правовые основы обеспечения национальной безопасности Российской Федерации.

Уметь:

- использовать в практической деятельности правовые знания;

- анализировать и составлять правовые акты и осуществлять правовую оценку информации, используемых в профессиональной деятельности, предпринимать необходимые меры по восстановлению нарушенных прав.

Владеть:

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

2.6.

4. Содержание дисциплины

№ п/п	Наименование раздела дисциплины
1.	Правоведение как учебная дисциплина
2.	Механизм государства
3.	Форма государства
4.	Понятие права. Нормы права. Система права
5.	Формы права
6.	Правоотношения. Реализация норм права
7.	Правонарушения и юридическая ответственность
8.	Основы Конституционного права России
9.	Общая характеристика административного права России
10.	Общая характеристика уголовного и уголовно-процессуального права России
11.	Основы гражданского права России
12.	Система обеспечения национальной безопасности Российской Федерации

Аннотация рабочей программы учебной дисциплины «Экономика»

1. Цели и задачи дисциплины

Формирование у студента экономического мышления, понимания сущности экономических процессов, происходящих в обществе, овладение теоретическими и методологическими основами оценки проблем экономической безопасности; введение в круг основных экономических категорий, законов и закономерностей.

Изучение дисциплины направлено на глубокое понимание выпускниками основных экономических законов и закономерностей развития общества; привитие им

навыков самостоятельного анализа экономических процессов и явлений и оценки их влияния на состояние национальной безопасности России.

2. Место дисциплины в структуре ООП

«Экономика» является дисциплиной ГСЭ. Специальных требований к входным знания, умениям и компетенциям обучаемых не предусматривается. Она выступает в качестве теоретической и методологической основы для специальных экономических дисциплин, (например «Экономическая безопасность», «Финансы, денежное обращение и кредит», «Налоговая система и налогообложение», «Финансовый анализ») если таковые предусмотрены учебным планом.

3. Требования к уровню освоения дисциплины

В результате изучения дисциплины «Экономика» студенты должны **овладеть следующими компетенциями:**

- 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-4);
- 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 и обоснования проектных решений по обеспечению информационной безопасности (ПК-13).

Знать:

- основные экономические категории и закономерности, методы анализа экономических явлений и процессов, специфические черты функционирования хозяйственной системы на (микро- и макро-) уровнях, основные понятия экономической и финансовой деятельности отрасли и ее структурных подразделений.

Уметь:

- оценивать эффективность управленческих решений и анализировать экономические показатели деятельности подразделения.

4. Содержание дисциплины

№ п/п	Наименование раздела дисциплины
1.	Предмет экономики как науки. Основные закономерности экономической организации общества.
2.	Рынок и механизм его функционирования.
3.	Монополизм в экономике и антимонопольная политика государства.
4.	Рынки факторов производства и факторные доходы.
5.	Национальная экономика и основные макроэкономические показатели.
6.	Государство в рыночной экономике.
7.	Макроэкономическое равновесие. Цикличность развития рыночной экономики и экономический рост.
8.	Деньги, инфляция и антиинфляционная политика государства.
9.	Финансы и бюджетно-налоговая политика государства.
10.	Кредит и кредитная система государства.
11.	Мировая экономика и международные экономические отношения.
12.	Глобализация экономики и проблемы обеспечения экономической безопасности страны.

Аннотация рабочей программы дисциплины
«АЛГЕБРА И ГЕОМЕТРИЯ»

1. Цели и задачи дисциплины

Дисциплина "Алгебра и геометрия" реализует требования федерального государственного образовательного стандарта высшего профессионального образования по направлению подготовки 090303 “Информационная безопасность автоматизированных систем”.

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

Дисциплина "Алгебра и геометрия" относится к числу фундаментально-прикладных математических дисциплин в силу отбора изучаемого материала и его важности для подготовки специалиста. Во всех разделах дисциплины большое внимание уделяется построению алгоритмов для решения практических задач.

Задачами дисциплины являются:

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

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

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

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

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

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

Таким образом, дисциплина "Алгебра и геометрия" является неотъемлемой составной частью профессиональной подготовки по направлению подготовки 090303 “Информационная безопасность автоматизированных систем”. Вместе с другими дисциплинами цикла математических и естественнонаучных дисциплин изучение данной дисциплины призвано формировать специалиста, и в частности, вырабатывать у него такие качества, как:

- строгость в суждениях и стремление к теоретическим обоснованиям,
- критическое отношение к результатам, пока они не доказаны,
- творческое мышление и стремление к научному поиску,
- организованность, трудолюбие и работоспособность,
- дисциплинированность и ответственность,
- самостоятельность и добросовестность.

2. Место дисциплины в структуре ООП

Дисциплина «Алгебра и геометрия» относится к числу дисциплин базовой части математического и естественнонаучного цикла.

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

– Знания, умения и навыки сформированные в процессе изучения программы общеобразовательной школы.

Дисциплина имеет разносторонние связи со многими другими математическими и профессиональными дисциплинами. Дисциплина основывается на знании числовых систем и функций, изученных в средней школе, а также в нескольких первых темах курса «Математический анализ». При изучении линейных пространств в алгебре широко используются знания, умения и наглядные представления, полученные студентами при изучении прямой и плоскости в аналитической геометрии. При изучении многочленов в алгебре используется доказываемая в теории функций комплексного переменного теорема о корнях многочленов над полем комплексных чисел.

С другой стороны, полученные в алгебре знания по конечномерным пространствам над произвольными полями служат базой для изучения действительных и комплексных пространств в курсе «Математический анализ». Знания из алгебры по теории многочленов, колец и групп широко используются в курсе «Математическая логика и теория алгоритмов» при изучении булевых и многозначных функций, а также в дисциплине «Дискретная математика».

Знания, полученные при изучении дисциплины «Алгебра и геометрия», используются при изучении следующих дисциплин:

- Математический анализ
- Дискретная математика
- Математическая логика и теория алгоритмов
- Теория вероятностей и математическая статистика
- Теория информации
- Технологии и методы программирования
- Криптографические методы защиты информации
- Физика

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

способность понимать социальную значимость своей будущей профессии, цели и смысл государственной службы, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности, защиты интересов личности, общества и государства, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства (ОК-5);

способность логически верно, аргументировано и ясно строить устную и письменную речь на русском языке, готовить и редактировать тексты профессионального назначения, публично представлять собственные и известные научные результаты, вести дискуссии (ОК-7);

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

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

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

способность применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ПК-5);

способность осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере своей профессиональной деятельности (ПК-9);

способность применять современные методы исследования с использованием компьютерных технологий (ПК-10);

В результате изучения дисциплины студент должен:

Знать:

- возможности координатного метода для исследования различных геометрических объектов,
- основные задачи векторной алгебры и аналитической геометрии,
- основные виды уравнений простейших геометрических объектов,
- основные свойства важнейших алгебраических структур,
- основы линейной алгебры над произвольными полями,
- векторные пространства над полями и их свойства

Уметь:

- строить и изучать математические модели конкретных явлений и процессов для решения расчетных и исследовательских задач,
- определять возможности применения теоретических положений и методов математических дисциплин для постановки и решения конкретных прикладных задач,
- исследовать простейшие геометрические объекты по их уравнениям в различных системах координат,
- оперировать с числовыми и конечными полями, многочленами, матрицами,
- решать основные задачи линейной алгебры, в частности системы линейных уравнений над полями

Владеть:

- навыками использования методов аналитической геометрии и векторной алгебры в смежных дисциплинах и физике,
- методами линейной алгебры.

4. Содержание дисциплины

Раздел 1. Аналитическая геометрия

Тема № 1. Введение.

Тема № 2. Некоторые сведения из теории определителей и систем линейных уравнений.

Тема № 3. Векторная алгебра.

Тема № 4. Системы координат и простейшие задачи, решаемые с использованием векторной алгебры.

Тема № 5. Прямая линия на плоскости.

Тема № 6. Линии второго порядка на плоскости.

Тема № 7. Прямая и плоскость в пространстве.

Тема № 8. Поверхности второго порядка.

Раздел 2. Основы алгебры

Тема № 9. Основные алгебраические структуры.

Тема № 10. Матрицы над кольцами.

Тема № 11. Определители матриц. Обратимые матрицы.

Тема № 12. Матрицы над полями и системы линейных уравнений.

Тема № 13. Линейная зависимость векторов арифметических пространств.
Тема № 14. Подпространства арифметических пространств.
Тема № 15. Числовые кольца и поля.
Тема № 16. Кольца вычетов.
Тема № 17. Кольца многочленов.
Тема № 18. Линейные пространства.
Тема № 19. Линейные преобразования линейных пространств.
Тема № 20. Подобие матриц над полем.
Тема № 21. Линейные преобразования евклидовых пространств.

Аннотация рабочей программы дисциплины
«Математический анализ»

1. Цели и задачи дисциплины: Учебная дисциплина «Математический анализ» реализует требования федерального государственного образовательного стандарта высшего профессионального образования по направлению подготовки (специальности) 090303 «Информационная безопасность автоматизированных систем».

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

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

Учебная дисциплина «Математический анализ» является составной частью профессионального образования по направлению подготовки (специальности) 090303 «Информационная безопасность автоматизированных систем».

2. Место дисциплины в структуре ООП: «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.

Для успешного усвоения данной дисциплины необходимо, чтобы обучаемый владел знаниями, умениями и навыками, сформированными в процессе изучения математики в средней школе, а также дисциплины «Алгебра и геометрия».

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

«Физика»;

«Теория вероятностей и математическая статистика»;

«Теория информации».

Учебная дисциплина «Математический анализ» составит основу и для циклов дисциплин специализаций.

3. Требования к результатам освоения дисциплины:

Процесс изучения дисциплины направлен на формирование следующих компетенций:

способность логически верно, аргументировано и ясно строить устную и письменную речь на русском языке, готовить и редактировать тексты профессионального назначения, публично представлять собственные и известные научные результаты, вести дискуссии (ОК-7);

способность к логически-правильному мышлению, обобщению, анализу, критическому осмыслению информации, систематизации, прогнозированию, постановке исследо-

вательских задач и выбору путей их решения на основании принципов научного познания (ОК-9);

способность самостоятельно применять методы и средства познания, обучения и самоконтроля для приобретения новых знаний и умений, в том числе в новых областях, непосредственно не связанных со сферой деятельности, развития социальных и профессиональных компетенций, изменения вида своей профессиональной деятельности (ОК-10);

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

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

способность использовать языки, системы и инструментальные средства программирования в профессиональной деятельности (ПК-3);

способность применять достижения современных информационных технологий для поиска и обработки больших объемов информации по профилю деятельности в глобальных компьютерных системах, сетях, в библиотечных фондах и в иных источниках информации (ПК- 4);

способность применять современные методы исследования с использованием компьютерных технологий (ПК-10);

В результате изучения дисциплины обучаемый должен:

Знать:

основные положения теории пределов и непрерывных функций, теории числовых и функциональных рядов,

основные теоремы дифференциального и интегрального исчисления функций одной и нескольких переменных.

основные понятия теории функций комплексной переменной;

основные методы решения простейших дифференциальных уравнений и систем дифференциальных уравнений;

Уметь:

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

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

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

Владеть:

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

навыками решения задач с применением аппарата теории функций комплексной переменной;

навыками использования стандартных методов решения типовых дифференциальных уравнений;

навыками пользования библиотеками прикладных программ для решения прикладных математических задач;

4. Содержание дисциплины

Раздел 1. Действительные функции и пределы.

Тема 1. Действительные числа. Понятие функции.

Тема 2. Теория пределов числовых последовательностей и числовых рядов.

Тема 3. Теория пределов функций одной действительной переменной.

Тема 4. Непрерывность функций одной действительной переменной.

Тема 5. Дифференциальное исчисление функций одной действительной переменной.

Тема 6. Приложения дифференциального исчисления функций одной действительной переменной.

Раздел 2. Функции многих действительных переменных.

Тема 7. Теория пределов, непрерывность.

Тема 8. Дифференцируемость функции многих действительных переменных.

Раздел 3. Интегральное исчисление.

Тема 9. Неопределенный интеграл.

Тема 10. Определенный интеграл.

Тема 11. Кратные интегралы.

Тема 12. Криволинейные и поверхностные интегралы.

Раздел 4. Основные понятия теории функций комплексной переменной.

Тема 13. Введение.

Тема 14. Дифференцирование и интегрирование функций комплексной переменной.

Раздел 5. Дифференциальные уравнения.

Тема 15. Дифференциальные уравнения 1-го порядка.

Тема 16. Линейные дифференциальные уравнения n-го порядка.

Раздел 6. Элементы теории функциональных рядов.

Тема 17. Функциональные последовательности и ряды в действительной области.

Тема 18. Функциональные ряды в комплексной области.

Тема 19. Теория вычетов.

Тема 20. Ряды Фурье. Преобразование и интеграл Фурье.

Заключение

Аннотация рабочей программы дисциплины «ДИСКРЕТНАЯ МАТЕМАТИКА»

1. Цели и задачи дисциплины

Дисциплина "Дискретная математика" реализует требования федерального государственного образовательного стандарта высшего профессионального образования по специальности 090303 “Информационная безопасность автоматизированных систем”.

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

Дисциплина "Дискретная математика" относится к числу фундаментальных математических дисциплин в силу отбора изучаемого материала и его важности для подготовки специалиста.

Задачи дисциплины:

воспитание у студентов математической и технической культуры,

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

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

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

Таким образом, дисциплина "Дискретная математика" является неотъемлемой составной частью профессиональной подготовки по направлению подготовки 090303 “Информационная безопасность автоматизированных систем”. Вместе с другими дисциплинами математического и естественнонаучного цикла изучение данной дисциплины призвано формировать специалиста, и в частности, вырабатывать у него такие качества, как:

строгость в суждениях,

творческое мышление,

организованность и работоспособность,

дисциплинированность,

самостоятельность и ответственность.

2. Место дисциплины в структуре ООП

Дисциплина «Дискретная математика» относится к числу дисциплин базовой части математического и естественнонаучного цикла.

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

«Математический анализ» – основы теории пределов и действительных функций одного переменного;

«Алгебра и геометрия» – основы общей и линейной алгебры.

Знания, полученные студентами в ходе изучения дисциплины "Дискретная математика", используются при изучении дисциплин:

Математическая логика и теория алгоритмов

Теория вероятностей и математическая статистика

Теория информации

Технологии и методы программирования

Криптографические методы защиты информации

Сети и системы передачи информации,

Техническая защита информации,

3. Требования к результатам освоения дисциплины:

Процесс изучения дисциплины направлен на формирование следующих компетенций:

способность понимать социальную значимость своей будущей профессии, цели и смысл государственной службы, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства (ОК-5);

способность логически верно, аргументировано и ясно строить устную и письменную речь на русском языке, готовить и редактировать тексты профессионального назначения, публично представлять собственные и известные научные результаты, вести дискуссии (ОК-7);

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

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

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

способность применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ПК-5).

способность осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере своей профессиональной деятельности (ПК-9);

способность применять современные методы исследования с использованием компьютерных технологий (ПК-10);

В результате изучения дисциплины студент должен:

Знать:

основы комбинаторного анализа;

метод включения-исключения; производящие функции;

основные понятия теории автоматов;

основные понятия и алгоритмы теории графов;

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

методы перечисления для основных дискретных структур;

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

Уметь:

применять стандартные методы дискретной математики и теории автоматов для решения профессиональных задач;

решать задачи периодичности и эквивалентности для конечных автоматов;

применять аппарат производящих функций и рекуррентных соотношений для решения перечислительных задач;

решать оптимизационные задачи на графах;

Владеть:

навыками построения дискретных моделей при решении профессиональных задач;

навыками применения языка и средств дискретной математики;

навыками решения комбинаторных и теоретико-графовых задач.

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

4. Содержание дисциплины

Раздел 1. Основы комбинаторики

Тема № 1. Введение.

Тема 2. Основы комбинаторики.

Тема 3. Бинарные отношения.

Тема 4. Метод включения-исключения.

Тема 5. Метод производящих функций.

Раздел 2. Элементы теории графов

Тема 6. Основные понятия теории графов

Тема 7. Эйлеровы и гамильтоновы графы

Тема 8. Деревья

Тема 9. Метрические характеристики графа

Тема 10. Укладки и раскраски

Раздел 3. Элементы теории кодирования

Тема 11. Основные понятия

Тема 12. Линейные коды

Тема 13. Коды Хэмминга и циклический

Раздел 4. Конечные автоматы

Тема 14. Основные понятия теории автоматов.

Тема 15. Линейные автоматы над конечным полем.

Тема 16. Эксперименты по распознаванию состояний автоматов.

Аннотация рабочей программы дисциплины
МАТЕМАТИЧЕСКАЯ ЛОГИКА И ТЕОРИЯ АЛГОРИТМОВ

1. Цели и задачи дисциплины

Дисциплина "Математическая логика и теория алгоритмов" реализует требования федерального государственного образовательного стандарта высшего профессионального образования по направлению подготовки 090303 “Информационная безопасность автоматизированных систем”, содействует фундаментализации образования, формированию мировоззрения и развитию логического мышления.

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

Задачами дисциплины являются:

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

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

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

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

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

Таким образом, дисциплина "Математическая логика и теория алгоритмов" является неотъемлемой составной частью профессиональной подготовки по направлению подготовки 090303 “Информационная безопасность автоматизированных систем”. Изучение данной дисциплины призвано формировать специалиста, и в частности, вырабатывать у него такие качества, как:

строгость в суждениях,
творческое мышление,
организованность и работоспособность,
дисциплинированность,
самостоятельность и ответственность.

2. Место дисциплины в структуре ООП

Дисциплина "Математическая логика и теория алгоритмов" относится к числу дисциплин базовой части математического и естественнонаучного цикла. Дисциплина основывается на знаниях, полученных при изучении дисциплин

«Математический анализ» – основы теории пределов и действительных функций одного переменного;

«Алгебра и геометрия» – основы общей и линейной алгебры,

«Дискретная математика» – основы комбинаторики и теории графов.

Знания, полученные при изучении дисциплины "Математическая логика и теория алгоритмов", используются при изучении дисциплин

Технологии и методы программирования,

Безопасность систем баз данных,

Криптографические методы защиты информации,

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

способность понимать социальную значимость своей будущей профессии, цели и смысл государственной службы, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства (ОК-5);

способность логически верно, аргументировано и ясно строить устную и письменную речь на русском языке, готовить и редактировать тексты профессионального назначения, публично представлять собственные и известные научные результаты, вести дискуссии (ОК-7);

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

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

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

способность применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ПК-5).

способность осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере своей профессиональной деятельности (ПК-9);

способность применять современные методы исследования с использованием компьютерных технологий (ПК-10);

В результате изучения дисциплины студент должен

Знать

основные понятия математической логики и теории алгоритмов;

язык и средства современной математической логики,

представления булевых функций и способы минимизации формул;

типовые свойства и способы задания функций многозначной логики.

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

подходы к оценкам сложности алгоритмов,

методы построения эффективных алгоритмов,

возможности применения общих логических принципов в математике и профессиональной деятельности,

Уметь

находить и исследовать свойства представлений булевых и многозначных функций формулами в различных базисах;

оценивать сложность алгоритмов и вычислений;

классифицировать алгоритмы по классам сложности.

применять методы математической логики и теории алгоритмов к решению задач математической кибернетики,

Владеть

навыками использования языка современной символической логики;

навыками применения методов и фактов теории алгоритмов, относящимися к решению переборных задач.

навыками упрощения формул алгебры высказываний и алгебры предикатов

навыками составления программ на машинах Тьюринга

4. Содержание дисциплины

РАЗДЕЛ 1. АЛГЕБРА ЛОГИКИ

Тема 1. Введение

Тема 2. Алгебра высказываний и алгебра предикатов

Тема 3. Булевы функции и их обобщение

РАЗДЕЛ 2. ЛОГИЧЕСКИЕ ИСЧИСЛЕНИЯ

Тема 4. Исчисление высказываний

Тема 5. Исчисление предикатов

Тема 6. Метод резолюций

РАЗДЕЛ 3. АЛГОРИТМИЧЕСКИЕ МОДЕЛИ

Тема 7. Элементы теории алгоритмов

Тема 8. Алгоритмическая разрешимость и неразрешимость

РАЗДЕЛ 4. СЛОЖНОСТЬ АЛГОРИТМОВ

Тема 9. Сложность алгоритмов и вычислений

Тема 10. Методы построения эффективных алгоритмов.

Тема 11. Сложностная классификация переборных задач

Тема 12. Теория алгоритмов и задачи использования ЭВМ

Аннотация рабочей программы дисциплины
«Информатика»

1. Цели и задачи дисциплины

Целью изучения дисциплины «Информатика» является формирование общей информационной культуры студентов, подготовка их к деятельности, связанной с использованием современных информационных технологий.

Задачи дисциплины:

изучение основных понятий информатики;

изучение свойств и способов записи алгоритмов;

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

ознакомление с логическими основами устройства ЭВМ;

ознакомление с составом и назначением функциональных узлов компьютера;

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

изучение основ программирования в командных оболочках;

овладение навыками применения сервисных программных средств системного и прикладного назначения;

изучение основ построения компьютерных сетей;

овладение навыками поиска информации в глобальной информационной сети Интернет.

2. Место дисциплины в структуре ООП

Дисциплина "Информатика" в основной образовательной программе подготовки бакалавров находится в учебном блоке математических и естественнонаучных дисциплин.

Для успешного усвоения данной дисциплины необходимо, чтобы студент владел знаниями, умениями и навыкамив объеме требований «СТАНДАРТА СРЕДНЕГО (ПОЛНОГО) ОБЩЕГО ОБРАЗОВАНИЯ ПО ИНФОРМАТИКЕ И ИКТ» Минобразования России от 05.03.04 №1089.

Дисциплина "Информатика" является предшествующей для изучения следующих дисциплин: «Языки программирования», «Организация ЭВМ и вычислительных систем», «Основы информационной безопасности», «Безопасность операционных систем», «Безопасность сетей ЭВМ».

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

способность логически верно, аргументировано и ясно строить устную и письменную речь на русском языке, готовить и редактировать тексты профессионального назначения, публично представлять собственные и известные научные результаты, вести дискуссии (ОК-7);

способность понимать сущность и значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска и обработки больших объемов информации по профилю деятельности в глобальных компьютерных системах, сетях, в библиотечных фондах и в иных источниках информации (ПК-3);

способность работать с программными средствами прикладного, системного и специального назначения (ПК-8).

В результате изучения дисциплины студент должен

знать:

основные понятия информатики;

формы и способы представления данных в персональном компьютере;

состав, назначение функциональных компонентов и программного обеспечения персонального компьютера;

классификацию современных компьютерных систем;

типовые структуры и принципы организации компьютерных сетей;

уметь:

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

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

владеть:

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

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

4. Содержание дисциплины

Раздел 1. Основные понятия информатики

Тема 1. Введение в дисциплину

Тема 2. Кодирование, измерение и защита информации

Раздел 2. Основы построения ЭВМ

Тема 3. Арифметические основы ЭВМ

Тема 4. Логические основы ЭВМ

Тема 5. Архитектура и организация ЭВМ

Раздел 3. Программное обеспечение ЭВМ

Тема 6. Программное обеспечение информационных систем

Тема 7. Введение в операционные системы

Тема 8. Введение в файловые системы

Тема 9. Командные оболочки

Раздел 4. Компьютерные сети

Тема 10. Введение в компьютерные сети
Тема 11. Основы Internet

Аннотация рабочей программы дисциплины
«Языки программирования»

1. Цели и задачи дисциплины

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

Задачи дисциплины:

ознакомление с теоретическими основами программирования;

изучение основ алгоритмизации;

изучение средств описания данных и средств описания действий языков программирования;

овладение навыками программирования;

освоение современных сред создания программных продуктов.

2. Место дисциплины в структуре ООП

Дисциплина «Языки программирования» относится к числу дисциплин базовой части профессионального цикла.

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

«Информатика» – уметь пользоваться сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети Интернет; владеть навыками работы с офисными приложениями;

«Английский язык» – владеть иностранным языком в объеме, необходимом для получения и изложения информации по профессиональной тематике.

Дисциплина "Языки программирования" является предшествующей для изучения следующих базовых дисциплин: «Технологии и методы программирования», «Программно-аппаратные средства обеспечения информационной безопасности».

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

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

способность использовать языки, системы и инструментальные средства программирования в профессиональной деятельности (ПК-3);

способность к освоению новых образцов программных, технических средств и информационных технологий (ПК-8);

способность разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ (ПК16);

способность участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности (ПК-18).

В результате изучения дисциплины студент должен

знать:

области и особенности применения языков программирования высокого уровня;

язык программирования высокого уровня (объектно-ориентированное программирование);

возможности, классификацию и область применения макрообработки;

способы обработки исключительных ситуаций;

особенности параллельного программирования, способы реализации взаимного исключения;

уметь:

работать с интегрированной средой разработки программного обеспечения;

реализовывать на языке высокого уровня алгоритмы решения профессиональных задач, в том числе задач обработки битовых потоков;

использовать шаблоны классов;

использовать шаблоны классов и средства макрообработки;

использовать динамически подключаемые библиотеки;

реализовывать основные структуры данных и базовые алгоритмы средствами языков программирования;

использовать в разрабатываемых программах возможности многопоточной обработки;

владеть:

навыками разработки, документирования, тестирования и отладки программ.

навыками программирования на языке программирования высокого уровня;

навыками использования средств синхронизации потоков MS Windows.

4. Содержание дисциплины

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

Тема 1. Общая характеристика языков программирования

Тема 2. Базовые понятия языка

Тема 3. Указатели, ссылки, массивы

Тема 4. Функции

Тема 5. Типы данных, определяемые пользователем

Тема 6. Ввод –вывод. Работа с файлами

Тема 7. Препроцессорные средства

Тема 8. Операции с разрядами

Тема 9. Межпроцессное взаимодействие. Параллельное программирование.

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

Тема 10. Основные принципы объектно-ориентированного программирования

Тема 11. Классы и объекты

Раздел 3. Основы объектно-ориентированного программирования. Язык C++

Тема 12. Перегрузка операций

Тема 13. Наследование

Тема 14. Виртуальные функции и полиморфизм

Тема 15. Шаблоны классов

Тема 16. Потоковый ввод-вывод

Тема 17. Обработка исключительных ситуаций

Тема 18. Стандартная библиотека шаблонов (STL)

Тема 19. Приложения с графическим интерфейсом пользователя

Аннотация рабочей программы дисциплины «Технологии и методы программирования»

1. **Цели и задачи дисциплины**

Целью изучения дисциплины «Технологии и методы программирования» является изучение современных технологий и методов программирования, получение навыков

проектирования и разработки программного обеспечения (ПО), расширение кругозора в сфере разработки ПО.

Задачи дисциплины:

изучение методологии и средств разработки ПО;

изучение методов проектирования ПО;

изучение оценки качества программного обеспечения;

изучение тестирования и отладки программного обеспечения;

изучение принципов, методов и средств сопровождения ПО;

изучение структур данных;

изучение алгоритмов и навыков их практической реализации при разработке программных систем.

2. Место дисциплины в структуре ООП

Дисциплина "Технологии и методы программирования" относится к числу дисциплин базовой части профессионального цикла.

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

«Языки программирования» – знать язык программирования высокого уровня (объектно-ориентированное программирование), уметь разрабатывать программы на языке программирования высокого уровня, уметь работать с современными интегрированными средами разработки программного обеспечения, владеть навыками программирования на языке программирования высокого уровня;

«Математическая логика и теория алгоритмов» – знать основные понятия теории автоматов, знать основные дискретные структуры: конечные автоматы, грамматики, графы, комбинаторные структуры, знать основные понятия теории сложности алгоритмов, уметь оценивать сложность алгоритмов и вычислений, владеть способами оценки сложности работы алгоритмов;

«Теория вероятностей и математическая статистика» – владеть навыками использования стандартных теоретико-вероятностных и статистических методов при решении прикладных задач;

«Информатика» – знать формы и способы представления данных в персональном компьютере, владеть навыками применения математического аппарата для решения прикладных теоретико-информационных задач.

Дисциплина "Технологии и методы программирования" обеспечивает изучение следующих дисциплин: «Разработка и эксплуатация защищенных автоматизированных систем», а также дисциплин вариативной части профессионального цикла, предусмотренных примерным учебным планом.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

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

способность использовать языки, системы и инструментальные средства программирования в профессиональной деятельности (ПК-3);

способность применять достижения современных информационных технологий для поиска и обработки больших объемов информации по профилю деятельности в глобальных компьютерных системах, сетях, в библиотечных фондах и в иных источниках информации (ПК-4);

способность к освоению новых образцов программных, технических средств и информационных технологий (ПК-8);

способность осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере своей профессиональной деятельности (ПК-9);

способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем (ПК-15);

способность разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ (ПК-16);

способность участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности (ПК-18);

способность участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности (ПК-19);

способность организовывать работу малых коллективов исполнителей, находить и принимать управленческие решения в сфере профессиональной деятельности (ПК-27);

В результате изучения дисциплины студент должен

знать:

современные технологии и методы программирования;

показатели качества программного обеспечения;

методологии и методы проектирования программного обеспечения;

методы тестирования и отладки ПО;

принципы организации документирования разработки, процесса сопровождения программного обеспечения;

основные структуры данных и способы их реализации на языке программирования;

основные комбинаторные и теоретико-графовые алгоритмы, а также способы их эффективной реализации и оценки сложности;

уметь:

формировать требования и разрабатывать внешние спецификации для разрабатываемого программного обеспечения;

планировать разработку сложного программного обеспечения;

проектировать структуру и архитектуру программного обеспечения с использованием современных методологий и средств автоматизации проектирования программного обеспечения;

проводить комплексное тестирование и отладку программных систем;

проектировать и кодировать алгоритмы с соблюдением требований к качественному стилю программирования;

реализовывать основные структуры данных и базовые алгоритмы средствами языков программирования;

проводить выбор эффективных способов реализации структур данных и конкретных алгоритмов при решении профессиональных задач;

работать с интегрированной средой разработки программного обеспечения;

владеть:

навыками проектирования программного обеспечения с использованием средств автоматизации;

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

навыками разработки программной документации;

навыками программирования с использованием эффективных реализаций структур данных и алгоритмов.

5. Содержание дисциплины

Раздел 1. Технология программирования

Тема 1. Жизненный цикл ПО, методологии и стандарты разработки ПО

Тема 2. Планирование и организация разработки ПО

Тема 3. Проектирование ПО

Тема 4. Основы объектно-ориентированного анализа и проектирования ПО

Тема 5. Кодирование ПО

Тема 6. Технологии разработки распределенных программных систем. Перспективы развития технологий программирования

Тема 7. Тестирование и отладка ПО

Тема 8. Документирование ПО

Тема 9. Сопровождение ПО

Раздел 2. Методы программирования

Тема 10. Методы анализа алгоритмов

Тема 11. Динамические структуры данных

Тема 12. Поиск и сортировка

Тема 13. Основные алгоритмы на графах

Аннотация рабочей программы дисциплины «Электроника и схемотехника»

1. **Цели и задачи дисциплины**

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

Задачи дисциплины:

изучение основных элементов теории электрических цепей;

изучение принципов работы базовых аналоговых и цифровых электронных схем;

изучение схемотехнических подходов разработки основных аналоговых и цифровых узлов автоматизированных систем;

изучение методов анализа работы электронных схем;

изучение принципов применения современных электронных средств обеспечения информационной безопасности автоматизированных систем;

овладение методами разработки узлов автоматизированных систем на основе современной элементной базы.

2. Место дисциплины в структуре ООП

Дисциплина «Электроника и схемотехника» относится к числу дисциплин базовой части профессионального цикла.

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

«Физика» – знать основные законы электричества, магнетизма, основы теории колебаний и волн, физики твёрдого тела и владеть навыками проведения физического эксперимента и обработки его результатов;

«Инженерная графика» – знать основные положения стандартов Единой системы конструкторской документации и Единой системы программной документации, уметь применять требования Единой системы конструкторской документации и Единой системы программной документации при разработке технической документации;

«Математический анализ» – знать основные положения теории пределов и непрерывных функций, теории числовых и функциональных рядов, основные теоремы дифференциального и интегрального исчисления функций, а также уметь решать основные задачи на вычисление пределов функций, дифференцирование, интегрирование и разложение функций в ряды;

«Информатика» – знать системы счисления, способы представления данных в ЭВМ, состав и назначение функциональных компонентов и программного обеспечения компьютера, уметь пользоваться средствами поиска информации в сети Интернет.

Дисциплина "Электроника и схемотехника" является предшествующей для изучения следующих базовых дисциплин: «Сети и системы передачи информации», «Техническая защита информации», «Организация ЭВМ и вычислительных систем», «Разработка и эксплуатация защищенных автоматизированных систем», «Программно-аппаратные средства обеспечения информационной безопасности».

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

способность применять достижения современных информационных технологий для поиска и обработки больших объемов информации по профилю деятельности в глобальных компьютерных системах, сетях, в библиотечных фондах и в иных источниках информации (ПК 4);

способность к освоению новых образцов программных, технических средств и информационных технологий (ПК-8);

способность применять современные методы исследования с использованием компьютерных технологий (ПК-10);

способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем (ПК-15);

способность разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ (ПК-16);

способность участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности (ПК-18);

способность участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности (ПК-19);

способность участвовать в проектировании средств защиты информации и средств контроля защищенности автоматизированной системы (ПК-22).

В результате изучения дисциплины студент должен

знать:

основы теории электрических цепей;

принципы работы элементов и функциональных узлов электронной аппаратуры;

методы анализа и синтеза электронных схем;

типовые схемотехнические решения основных узлов и блоков электронной аппаратуры;

уметь:

применять на практике методы анализа электрических цепей;

работать с современной элементной базой электронной аппаратуры;

использовать стандартные методы и средства проектирования цифровых узлов и устройств, в том числе для средств защиты информации;

владеть:

навыками использования современной измерительной аппаратуры при экспериментальном исследовании электронной аппаратуры;

навыками работы с программными средствами схемотехнического моделирования;

навыками чтения принципиальных схем, построения временных диаграмм и восстановления алгоритма работы узла, устройства и системы по комплекту документации;

навыками оценки быстродействия и оптимизации работы электронных схем на базе современной элементной базы.

4. Содержание дисциплины

Раздел 1. Основы теории электрических цепей и сигналов

Тема 1. Основные определения и законы теории электрических цепей

Тема 2. Электрические цепи при гармоническом воздействии

Тема 3. Четырехполюсники, фильтры и длинные линии

Тема 4. Сигналы и их спектры

Раздел 2. Полупроводниковые приборы, усилители и аналоговые преобразователи

Тема 5. Полупроводниковые приборы

Тема 6. Электронные усилители

Тема 7. Нелинейное и параметрическое преобразование сигналов

Раздел 3. Схемотехника импульсных и цифровых устройств

Тема 8. Цифровая схемотехника

Тема 9. Триггеры

Тема 10. Функциональные узлы комбинационного и последовательностного типа

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

Тема 11. Схемотехника запоминающих устройств

Тема 12. Схемотехника устройств на базе программируемой логики

Раздел 5. Разработка и применение цифровых устройств

Тема 13. Функционирование цифровых элементов в составе узлов и блоков

Тема 14. Разработка и применение цифровых узлов и блоков

Аннотация рабочей программы дисциплины «Безопасность операционных систем»

1. Цели и задачи дисциплины

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

Задачи дисциплины:

изучение назначения и функций ОС;

приобретение навыков управления ресурсами и задачами в ОС;

освоение администрирования ОС;

изучение требований к защите ОС;

изучение методов и средств разграничения доступа в ОС;

изучение аудита в ОС;

формирование специальных теоретических и практических знаний, обеспечивающих возможность планирования политики безопасности ОС;

приобретение навыков эффективной и безопасной эксплуатацию ОС автоматизированных систем;

формирование специальных теоретических и практических знаний, обеспечивающих возможность проектировании средств защиты информации и средств контроля защищенности автоматизированных систем;

приобретение навыков эффективного применения информационно-технологических ресурсов ОС с учетом требований информационной безопасности;

приобретение навыков эффективного применения средств защиты информационно-технологических ресурсов ОС;

формирование специальных теоретических и практических знаний, позволяющих администрировать подсистему информационной безопасности автоматизированной системы;

формирование специальных теоретических и практических знаний, позволяющих обеспечить восстановление работоспособности систем защиты информации при возникновении нештатных ситуаций.

2. Место дисциплины в структуре ООП

Дисциплина «Безопасность операционных систем» относится к числу дисциплин базовой части профессионального цикла.

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

Изучение дисциплины «Безопасность операционных систем» базируется на следующих дисциплинах:

«Информатика» - знать формы и способы представления данных в персональном компьютере, классификацию современных компьютерных систем, типовые структуры и принципы организации компьютерных сетей; уметь применять типовые программные средства сервисного назначения (средства восстановления системы после сбоев, дефрагментации и очистки диска и т.п.), пользоваться сетевыми средствами и внешними носителями информации для обмена данными; владеть навыками обеспечения безопасности информации с помощью типовых программных средств (антивирусов, архиваторов, стандартных сетевых средств обмена информацией и т.п.), навыками поиска и обмена информацией в глобальной информационной сети Интернет;

«Языки программирования» - знать общие принципы построения и использования современных языков программирования высокого уровня, язык программирования высокого уровня (объектно-ориентированное программирование); уметь работать с интегрированной средой разработки программного обеспечения, использовать динамически подключаемые библиотеки; владеть навыками разработки, документирования, тестирования и отладки программного обеспечения в соответствии с современными технологиями и методами программирования.

«Основы информационной безопасности» - знать основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; уметь классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; владеть профессиональной терминологией в области информационной безопасности.

Дисциплина «Безопасность операционных систем» является предшествующей для изучения следующих базовых дисциплин: «Безопасность систем баз данных», «Разработка и эксплуатация защищенных автоматизированных систем», «Программно-аппаратные средства обеспечения информационной безопасности», «Организация ЭВМ и вычислительных систем».

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

способность использовать языки, системы и инструментальные средства программирования в профессиональной деятельности (ПК-3);

способность к освоению новых образцов программных, технических средств и информационных технологий (ПК-8);

способность проводить анализ защищенности автоматизированных систем (ПК-12);

способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы (ПК-13);

способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем (ПК-15);

способность участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности (ПК-18);

способность разрабатывать политики информационной безопасности автоматизированных систем (ПК-20);

способность участвовать в проектировании средств защиты информации и средств контроля защищенности автоматизированной системы (ПК-22);

способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации (ПК-33);

способность обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности (ПК-35);

способность обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы (ПК-36);

способность администрировать подсистему информационной безопасности автоматизированной системы (ПК-37);

способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы (ПК-38);

способность обеспечить восстановление работоспособности систем защиты информации при возникновении нештатных ситуаций (ПК-40).

В результате изучения дисциплины студент должен:

знать:

принципы построения и функционирования, примеры реализаций современных операционных систем;

функции ОС, основные концепции управления процессорами, памятью, вспомогательной памятью, устройствами;

критерии оценки эффективности и надежности средств защиты ОС;

принципы организации и структуру подсистем защиты ОС семейств UNIX и Windows;

уметь:

использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем;

оценивать эффективность и надежность защиты операционных систем;

планировать политику безопасности операционных систем;

владеть:

навыками работы с операционными системами семейств Windows и Unix, восстановления операционных систем после сбоев;

навыками установки и настройки операционных систем семейств Windows и Unix с учетом требований по обеспечению информационной безопасности.

4. Содержание дисциплины

Раздел 1. Основы функционирования ОС

Тема 1. Назначение и функции операционных систем

Тема 2. Управление задачами и ресурсами в ОС

Тема 3. Автоматизация решения задач администрирования в ОС с использованием языков сценариев

Раздел 2. Безопасность ОС
Тема 4. Требования к защите ОС
Тема 5. Разграничение доступа в ОС
Тема 6. Аудит в ОС

Аннотация рабочей программы дисциплины «Безопасность сетей ЭВМ»

1. **Цели и задачи дисциплины**

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

Задачи:

изучение основных элементов теории построения сетей;

изучение основных принципов функционирования сетевых протоколов;

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

изучение основных угроз в сетях ЭВМ и методов противодействия им;

овладение механизмами построения систем безопасности сетей ЭВМ.

2. Место дисциплины в структуре ООП

Дисциплина «Безопасность сетей ЭВМ» относится к числу дисциплин базовой части профессионального цикла.

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

«Информатика» – знать формы и способы представления данных в персональном компьютере, типовые структуры и принципы организации компьютерных сетей;

«Языки программирования» – знать язык программирования высокого уровня (объектно-ориентированное программирование), уметь работать с интегрированной средой разработки программного обеспечения, владеть навыками разработки, документирования, тестирования и отладки программного обеспечения в соответствии с современными технологиями и методами программирования;

«Основы информационной безопасности» – знать сущность и понятие информации, информационной безопасности и характеристику ее составляющих, источники и классификацию угроз информационной безопасности, основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации, владеть профессиональной терминологией в области информационной безопасности;

«Сети и системы передачи информации» – знать основные характеристики сигналов электросвязи, спектры и виды модуляции, принципы построения и функционирования систем и сетей передачи информации, способы кодирования информации, основные телекоммуникационные протоколы.

Дисциплина «Безопасность сетей ЭВМ» является предшествующей для изучения следующих базовых дисциплин: «Разработка и эксплуатация защищенных автоматизированных систем», «Организация ЭВМ и вычислительных систем», «Безопасность систем баз данных», «Программно-аппаратные средства обеспечения информационной безопасности».

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих профессиональных компетенций:

способность использовать языки, системы и инструментальные средства программирования в профессиональной деятельности (ПК-3);

способность применять достижения современных информационных технологий для поиска и обработки больших объемов информации по профилю деятельности в гло-

бальных компьютерных системах, сетях, в библиотечных фондах и в иных источниках информации (ПК-4);

способность к освоению новых образцов программных, технических средств и информационных технологий (ПК-8);

способность проводить анализ защищенности автоматизированных систем (ПК-12);

способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы (ПК-13);

способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем (ПК-15);

способность проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем (ПК-17);

способность участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности (ПК-18);

способность участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности (ПК-19);

способность разрабатывать политики информационной безопасности автоматизированных систем (ПК-20);

способность участвовать в проектировании средств защиты информации и средств контроля защищенности автоматизированной системы (ПК-22);

способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации (ПК-33);

способность обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности (ПК-35);

способность обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы (ПК-36);

способность администрировать подсистему информационной безопасности автоматизированной системы (ПК-37);

способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы (ПК-38);

способность обеспечить восстановление работоспособности систем защиты информации при возникновении нештатных ситуаций (ПК-40).

В результате изучения дисциплины студент должен:

знать:

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

основные протоколы сетей ЭВМ;

последовательность и содержание этапов построения компьютерных сетей;

эталонную модель взаимодействия открытых систем;

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

уметь:

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

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

проводить мониторинг угроз безопасности компьютерных сетей;

владеть:

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

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

навыками использования программно-аппаратных средств обеспечения безопасности сетей ЭВМ.

4. Содержание дисциплины

Раздел 1. Безопасность сетезависимых уровней

Тема 1. Основы организации и функционирования сетей ЭВМ

Тема 2. Физический и канальный уровень построения сетей ЭВМ

Тема 3. Технологии построения локальных сетей ЭВМ

Тема 4. Сетевой уровеннь построения сетей ЭВМ. Маршрутизация

Раздел 2. Безопасность сетенезависимых уровней

Тема 5. Транспортная подсистема сетей ЭВМ

Тема 6. Уровень приложений. Управление сетями ЭВМ

Тема 7. Программно-технические средства защиты сетей ЭВМ .

Аннотация рабочей программы дисциплины «Безопасность систем баз данных»

1. Цели и задачи дисциплины

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

В задачи дисциплины "Безопасность систем баз данных" входит формирование необходимого минимума специальных теоретических знаний и практических навыков по следующим аспектам:

проектирование баз данных;

разработка прикладных программ для систем баз данных;

эксплуатация систем баз данных;

обеспечение информационной безопасности систем баз данных.

2. Место дисциплины в структуре ООП

Дисциплина "Безопасность систем баз данных" относится к числу дисциплин базовой части профессионального цикла.

Для успешного усвоения данной дисциплины необходимо, чтобы студент владел знаниями и умениями, сформированными в процессе изучения дисциплин:

"Информатика" – знать формы и способы представления данных в персональном компьютере, уметь применять персональные компьютеры для обработки различных видов информации;

"Языки программирования" – знать язык программирования высокого уровня, уметь работать с интегрированной средой разработки программного обеспечения;

"Математическая логика и теория алгоритмов" – знать основные принципы математической логики, уметь преобразовывать формулы алгебры высказываний и формулы алгебры предикатов;

"Основы информационной безопасности" – знать сущность и понятие информационной безопасности и характеристику ее составляющих, источники и классификацию угроз информационной безопасности, основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации, уметь класси-

фицировать и оценивать угрозы информационной безопасности для объекта информатизации;

"Безопасность операционных систем" – знать функции ОС, основные концепции управления процессорами, памятью, вспомогательной памятью, устройствами, уметь использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем;

"Безопасность сетей ЭВМ" – принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей, уметь – эффективно использовать различные методы и средства защиты информации для компьютерных сетей.

Дисциплина "Безопасность систем баз данных" является предшествующей для изучения дисциплин "Разработка и эксплуатация защищенных автоматизированных систем" и "Программно-аппаратные средства обеспечения информационной безопасности", а также дисциплин вариативной части профессионального цикла, предусмотренных примерным учебным планом. Знания и практические навыки, полученные в ходе изучения данной дисциплины, используются обучаемыми при выполнении курсовых и дипломных работ.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины "Безопасность систем баз данных" направлен на формирование следующих профессиональных компетенций:

способность использовать языки, системы и инструментальные средства программирования в профессиональной деятельности (ПК-3);

способность применять достижения современных информационных технологий для поиска и обработки больших объемов информации по профилю деятельности в глобальных компьютерных системах, сетях, в библиотечных фондах и в иных источниках информации (ПК-4);

способность к освоению новых образцов программных, технических средств и информационных технологий (ПК-8);

способностью проводить анализ защищенности автоматизированных систем (ПК-12);

способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы (ПК-13);

способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем (ПК-15);

способность проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем (ПК-17);

способность участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности (ПК-18);

способность участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности (ПК-19);

способность разрабатывать политики информационной безопасности автоматизированных систем (ПК-20);

способность участвовать в проектировании средств защиты информации и средств контроля защищенности автоматизированной системы (ПК-22);

способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации (ПК-33);

способность формировать комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной системы (ПК-34);

способность обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности (ПК-35);

способность обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы (ПК-36);

способность администрировать подсистему информационной безопасности автоматизированной системы (ПК-37);

способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы (ПК-38);

способность обеспечить восстановление работоспособности систем защиты информации при возникновении нештатных ситуаций (ПК-40).

знать:

принципы построения и функционирования, примеры реализаций современных систем управления базами данных;

архитектуру систем баз данных;

основные модели данных;

физическую организацию баз данных;

средства обеспечения безопасности данных;

последовательность и содержание этапов проектирования баз данных;

уметь:

разрабатывать и администрировать базы данных;

реализовывать политику безопасности баз данных;

выделять сущности и связи предметной области;

отображать предметную область на конкретную модель данных;

нормализовывать отношения при проектировании реляционной базы данных;

создавать объекты базы данных;

выполнять запросы к базе данных;

разрабатывать прикладные программы, осуществляющие взаимодействие с базами данных;

применять средства обеспечения безопасности данных;

владеть:

навыками эксплуатации и администрирования баз данных с учетом требований по обеспечению информационной безопасности;

навыками разработки, документирования баз данных с учетом требований по обеспечению информационной безопасности.

4. Содержание дисциплины

Раздел 1. Основы систем баз данных

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

Тема 2. Основы теории баз данных

Тема 3. Реляционные базы данных

Тема 4. Проектирование баз данных

Тема 5. Физическая организация баз данных

Тема 6. Средства поддержания интерфейса с различными категориями пользователей

Раздел 2. Безопасность систем баз данных

Тема 7. Концепция безопасности баз данных

Тема 8. Средства обеспечения целостности баз данных

Тема 9. Средства обеспечения конфиденциальности баз данных

Тема 10. Аудит систем баз данных

Тема 11. Средства поддержки высокой готовности систем баз данных

Аннотация рабочей программы дисциплины
«Организация ЭВМ и вычислительных систем»

1. **Цели и задачи дисциплины**

Целью изучения дисциплины «Организация ЭВМ и вычислительных систем» является обеспечение обучаемых необходимым объемом знаний об основных понятиях в области ЭВМ и систем, классификации, базовых принципах построения и функционирования ЭВМ и систем, состоянии и перспективах развития вычислительной техники.

Задачи дисциплины:

изучение терминологии в области ЭВМ и ВС;

изучение классификации и показателей качества ЭВМ и ВС;

изучение структуры и принципов функционирования ЭВМ и ВС;

изучение архитектуры компонентов ЭВМ и ВС;

изучение архитектуры параллельных ЭВМ и ВС;

изучение перспективных направлений развития ЭВМ и ВС;

приобретение в ходе курсового проектирования практических навыков по разработке компонентов автоматизированных систем.

2. Место дисциплины в структуре ООП

Дисциплина «Организация ЭВМ и вычислительных систем» относится к числу дисциплин базовой части профессионального цикла.

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

«Физика» – знать основы теории колебаний и волн, оптики, основы квантовой физики и физики твёрдого тела; уметь решать типовые прикладные физические задачи; владеть методами теоретического исследования физических явлений и процессов;

«Теория вероятностей и математическая статистика» – знать основные понятия и методы теории вероятностей, теории случайных процессов и математической статистики; уметь применять стандартные методы и модели к решению типовых теоретико-вероятностных и статистических задач; владеть навыками использования стандартных теоретико-вероятностных и статистических методов при решении прикладных задач;

«Математическая логика и теория алгоритмов» – знать основные принципы математической логики, основные понятия теории сложности алгоритмов; уметь оценивать сложность алгоритмов и вычислений; владеть способами оценки сложности работы алгоритмов;

«Языки программирования» – знать язык программирования высокого уровня;

«Электроника и схемотехника» – знать типовые схемотехнические решения основных узлов и блоков электронной аппаратуры;

«Безопасность операционных систем» – знать принципы построения и функционирования, примеры реализаций современных операционных систем;

«Безопасность сетей ЭВМ» – знать принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей, эталонную модель взаимодействия открытых систем;

«Информатика» – знать формы и способы представления данных в персональном компьютере; уметь пользоваться сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети Интернет; владеть навыками работы с офисными приложениями.

Дисциплина «Организация ЭВМ и вычислительных систем» является предшествующей для изучения следующих базовых дисциплин: «Разработка и эксплуатация защищенных автоматизированных систем», «Программно-аппаратные средства обеспечения информационной безопасности», а также дисциплин вариативной части профессионального цикла, предусмотренных примерным учебным планом.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

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

способность применять достижения современных информационных технологий для поиска и обработки больших объемов информации по профилю деятельности в глобальных компьютерных системах, сетях, в библиотечных фондах и в иных источниках информации (ПК-4);

способность применять методологии научно-исследовательской и практической деятельности (ПК-5);

способность к освоению новых образцов программных, технических средств и информационных технологий (ПК-8);

способность осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере своей профессиональной деятельности (ПК-9);

способность разрабатывать и исследовать модели автоматизированных систем (ПК-11);

способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем (ПК-15);

способность участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности (ПК-19);

способность обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности (ПК-35);

способность обеспечить восстановление работоспособности систем защиты информации при возникновении нештатных ситуаций (ПК-40).

В результате изучения дисциплины студент должен

знать:

архитектуру, принципы функционирования, элементную базу современных компьютеров, вычислительных и телекоммуникационных систем;

терминологию, основные руководящие и регламентирующие документы в области ЭВМ, комплексов и систем;

технические характеристики, показатели качества ЭВМ и систем, методы их оценки и пути совершенствования;

уметь:

проводить анализ архитектуры и структуры ЭВМ и систем, оценивать эффективность архитектурно-технических решений, реализованных при построении ЭВМ и систем;

осуществлять сбор, обработку, анализ и систематизацию научно-технической информации в области ЭВМ и систем с применением современных информационных технологий;

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

владеть:

методиками оценки показателей качества и эффективности ЭВМ и вычислительных систем;

навыками работы с технической документацией на ЭВМ и вычислительные системы.

4. Содержание дисциплины

Раздел 1. Базовые сведения теории ЭВМ и ВС

Тема 1. Введение в дисциплину «Организация ЭВМ и вычислительных систем»

Тема 2. Базовые сведения теории ЭВМ и вычислительных систем

Раздел 2. Архитектура, структура и компоненты ЭВМ

Тема 3. Элементы и узлы ЭВМ

Тема 4. Архитектура памяти ЭВМ

Тема 5. Периферийные устройства ЭВМ

Тема 6. Архитектура микропроцессорных систем

Раздел 3. Параллельные ВС и перспективные направления развития ЭВМ и ВС

Тема 7. Архитектура и структура параллельных ВС

Тема 8. Заключение

Аннотация рабочей программы дисциплины «Техническая защита информации»

1. Цели и задачи дисциплины

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

Задачами дисциплины является изучение

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

2. Место дисциплины в структуре ООП:

Дисциплина «Техническая защита информации» относится к базовой части профессионального цикла. Изучение её базируется на следующих дисциплинах: «Математический анализ», «Физика», «Теория вероятностей и математическая статистика», «Электроника и схемотехника», «Основы информационной безопасности».

Дисциплина «Техническая защита информации» является базовой дисциплиной профессионального цикла и обеспечивает чтение дисциплины «Разработка и эксплуатация защищённых автоматизированных систем» и подготовку выпускной квалификационной работы.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

а) общекультурными (ОК):

- способностью к логическому мышлению, обобщению, анализу, критическому осмыслению информации, систематизации, прогнозированию, постановке исследователь-

ских задач и выбору путей их решения на основании принципов научного познания (ОК-9);

- способностью самостоятельно применять методы и средства познания, обучения и самоконтроля для приобретения новых знаний и умений, в том числе в новых областях, непосредственно не связанных со сферой профессиональной деятельности, развития социальных и профессиональных компетенций, к изменению вида своей профессиональной деятельности (ОК-10);

б) профессиональными (ПК):

общепрофессиональными

- способностью выявлять естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности, и применять соответствующий физико-математический аппарат для их формализации, анализа и выработки решения (ПК-1);
- способностью применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ПК-5);
- способностью использовать нормативные правовые акты в своей профессиональной деятельности (ПК- 6);
- способностью к освоению новых образцов программных, технических средств и информационных технологий (ПК-8);

в научно-исследовательской деятельности

- способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере своей профессиональной деятельности (ПК-9);
- способностью проводить анализ защищенности автоматизированных систем (ПК-12);
- способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы (ПК-13);
- способностью проводить анализ рисков информационной безопасности автоматизированной системы (ПК-14);

в проектно-конструкторской деятельности

- способностью участвовать в проектировании средств защиты информации и средств контроля защищенности автоматизированной системы (ПК-22);

в контрольно-аналитической деятельности

- способностью проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-23);
- способностью проводить инструментальный мониторинг защищенности автоматизированных систем (ПК-26);
- ***в организационно-управленческой деятельности***

- способностью организовать эксплуатацию автоматизированной системы с учетом требований информационной безопасности (ПК-30);

способностью разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, а также положений, инструкций и других организационно-распорядительных документов в сфере профессиональной деятельности (ПК-31);

способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации (ПК-33);

- способностью формировать комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной системы (ПК-34);

в эксплуатационной деятельности

- способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы (ПК-36);

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

знать:

- технические каналы утечки информации;
- возможности технических средств перехвата информации;
- способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации;
- организацию защиты информации от утечки по техническим каналам на объектах информатизации;
- основы физической защиты объектов информатизации;

уметь:

- пользоваться нормативными документами по противодействию технической разведке;
- анализировать и оценивать угрозы информационной безопасности объекта;

владеть:

- методами и средствами технической защиты информации;
- методами расчета и инструментального контроля показателей технической защиты информации.

4. Содержание дисциплины

Раздел 1. Технические каналы утечки информации

Тема 1. Основные понятия и определения

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

Тема 3. Технические каналы утечки акустической (речевой) информации

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

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

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

Раздел 3. Методы и средства контроля эффективности технической защиты информации

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

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

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

Раздел 4. Организация технической защиты информации

Тема 1. Основы физической защиты объектов информатизации

Тема 2. Организация технической защиты информации на объектах информатизации.

Аннотация рабочей программы дисциплины «Организационное и правовое обеспечение информационной безопасности»

1. Цели и задачи дисциплины

Учебная дисциплина «Организационное и правовое обеспечение информационной безопасности» («ОПО ИБ») является важной составляющей общей профессиональной подготовки специалистов в области обеспечения информационной безопасности. Она призвана обеспечить освоение слушателями практических навыков работы с нормативно-правовой базой деятельности в области обеспечения информационной безопасности автоматизированных систем.

2. Место дисциплины в структуре ООП

Дисциплина «Организационное и правовое обеспечение информационной безопасности» относится к числу дисциплин базовой части профессионального цикла.

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

«Правоведение» - основными правовыми понятиями;

«Основы информационной безопасности» - основными понятиями и терминологией в области обеспечения информационной безопасности.

В свою очередь, данная дисциплина является обеспечивающей для написания выпускной квалификационной работы.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

способность действовать в соответствии с Конституцией Российской Федерации, исполнять свой гражданский и профессиональный долг, руководствуясь принципами законности и патриотизма (ОК-1);

способность осуществлять свою деятельность в различных сферах общественной жизни с учетом принятых в обществе морально-нравственных и правовых норм, соблюдать принципы профессиональной этики (ОК-2);

способность понимать социальную значимость своей будущей профессии, цели и смысл государственной службы, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности, защиты интересов личности, общества и государства, готовность и способность к активной состязательной деятельности в условиях информационного противоборства (ОК-5);

способность к работе в многонациональном коллективе, к кооперации с коллегами, в том числе и над междисциплинарными, инновационными проектами, способность в качестве руководителя подразделения, лидера группы сотрудников формировать цели команды, принимать организационно-управленческие решения в ситуациях риска и нести за них ответственность, применять методы конструктивного разрешения конфликтных ситуаций (ОК-6);

способность логически верно, аргументировано и ясно строить устную и письменную речь на русском языке, создавать и редактировать тексты профессионального назначения, публично представлять собственные и известные научные результаты, вести дискуссии (ОК-7);

способность применять достижения современных информационных технологий для поиска и обработки больших объемов информации по профилю деятельности в глобальных компьютерных системах, сетях, в библиотечных фондах и в иных источниках информации (ПК – 4);

способность использовать нормативные правовые документы в своей профессиональной деятельности (ПК – 6);

способность применять основные методы, способы и средства получения, хранения, переработки и передачи информации, использовать компьютер как средство управления информацией (ПК-10);

способность осуществлять подбор, изучение и обобщение научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности телекоммуникационных систем (ПК-11);

способность разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности компьютерных систем, а также положений, инструкций и других организационно-распорядительных документов (ПК-18);

способность разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности телекоммуникационных систем, а также положений, инструкций и других организационно-распорядительных документов в сфере профессиональной деятельности (ПК-30).

В результате изучения дисциплины студенты должны:

знать:

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

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

организацию 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;

уметь:

применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности;

разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации;

владеть:

навыками работы с нормативными правовыми актами;

навыками организации и обеспечения режима секретности;

методами организации и управления деятельностью служб защиты информации на предприятии;

методами формирования требований по защите информации.

4. Содержание дисциплины

Раздел I. Правовое обеспечение информационной безопасности

Тема 1.1 Информационные отношения как объект правового регулирования. Законодательство Российской Федерации в области информационной безопасности

Тема 1.2. Правовой режим защиты государственной тайны

Тема 1.3. Правовые режимы защиты информации конфиденциального характера

Тема 1.4. Государственное регулирование деятельности в области защиты информации

Тема 1.5. Правовая охрана результатов интеллектуальной деятельности

Тема 1.6. Преступления в сфере компьютерной информации

Раздел II. Организационное обеспечение информационной безопасности

Тема 2.1. Понятие организационной защиты информации

Тема 2.2. Методы обеспечения физической безопасности

Тема 2.3. Технологические меры поддержания безопасности

Тема 2.4. Организация режима секретности

Тема 2.5. Допуск к государственной тайне

Тема 2.6. Защита компьютерной информации.

Аннотация рабочей программы дисциплины
«Программно-аппаратные средства обеспечения информационной безопасности»

1. Цели и задачи дисциплины

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

Задачи дисциплины:

изучение моделей угроз и модели нарушителя информационной безопасности автоматизированной системы;

изучение методов анализа проектных решений по обеспечению безопасности автоматизированных систем;

получение практических навыков проектирования средств защиты информации автоматизированной системы;

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

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

2. Место дисциплины в структуре ООП

Дисциплина «Программно-аппаратные средства обеспечения информационной безопасности» относится к числу дисциплин базовой части профессионального цикла.

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

«Языки программирования» – разрабатывать программы на языке программирования высокого уровня;

«Основы информационной безопасности» – основные средства и способы обеспечения информационной безопасности, подходы к построению систем защиты информации;

«Безопасность операционных систем» – использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем;

«Безопасность сетей ЭВМ» – эффективно использовать различные методы и средства защиты информации для компьютерных сетей;

«Безопасность систем баз данных» – уметь применять средства обеспечения безопасности данных, реализовывать политику безопасности баз данных, владеть навыками эксплуатации и администрирования баз данных с учетом требований по обеспечению информационной безопасности;

«Организация ЭВМ и вычислительных систем» – знать архитектуру, принципы функционирования, элементную базу современных компьютеров, вычислительных и телекоммуникационных систем, уметь анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем.

Дисциплина «Программно-аппаратные средства обеспечения информационной безопасности» является предшествующей для изучения следующих базовых дисциплин: «Управление информационной безопасностью».

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

способность использовать языки, системы и инструментальные средства программирования в профессиональной деятельности (ПК-3);

способность использовать нормативные и правовые документы в своей профессиональной деятельности (ПК- 6);

способность к освоению новых образцов программных, технических средств и информационных технологий (ПК-8);

способность проводить анализ защищенности автоматизированных систем (ПК-12);

способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы (ПК-13);

способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем (ПК-15);

способность проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем (ПК-17);

способность участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности (ПК-18);

способность участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности (ПК-19);

способность участвовать в проектировании средств защиты информации и средств контроля защищенности автоматизированной системы (ПК-22);

- способность проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-23);
- способность участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты автоматизированных систем (ПК-24);
- способность участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом требований к обеспечению информационной безопасности (ПК-25);
- способность проводить инструментальный мониторинг защищенности автоматизированных систем (ПК-26);

способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации (ПК-33);

способность обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы (ПК-36);

способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы (ПК-38);

В результате изучения дисциплины студент должен:

знать:

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

уметь:

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

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

владеть:

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

навыками использования программно-аппаратных средств обеспечения безопасности сетей ЭВМ.

4. Содержание дисциплины

Тема 1. Назначение и функции программно-аппаратных средств обеспечения безопасности

Тема 2. Методы защиты информации от несанкционированного доступа

Тема 3. Методы обеспечения целостности аппаратного обеспечения автоматизированных систем

Тема 4. Анализ уязвимости программного обеспечения автоматизированных систем

Тема 5. Методы защиты от вредоносных программ

Тема 6. Средства идентификация и аутентификации пользователей автоматизированных систем

Аннотация рабочей программы дисциплины «Разработка и эксплуатация защищенных автоматизированных систем»

1. Цели и задачи дисциплины

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

Задачи дисциплины:

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

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

изучение методов, способов и средств обеспечения отказоустойчивости автоматизированных систем;

изучение основных мер по защите информации в автоматизированных системах;

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

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

2. Место дисциплины в структуре ООП

Дисциплина «Разработка и эксплуатация защищенных автоматизированных систем» относится к числу дисциплин базовой части профессионального цикла подготовки по специальности «Информационная безопасность автоматизированных систем».

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

«Безопасность операционных систем» – знать критерии оценки эффективности и надежности средств защиты ОС, уметь использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных

систем, владеть навыками работы с операционными системами семейств Windows и Unix, восстановления операционных систем после сбоев;

«Безопасность сетей ЭВМ» – знать основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в сетях ЭВМ, уметь эффективно использовать различные методы и средства защиты информации для компьютерных сетей, проводить мониторинг угроз безопасности компьютерных сетей, владеть навыками использования программно-аппаратных средств обеспечения безопасности сетей ЭВМ;

«Основы информационной безопасности» – знать источники и классификацию угроз информационной безопасности, основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации, уметь классифицировать и оценивать угрозы информационной безопасности для объекта информатизации, владеть профессиональной терминологией в области информационной безопасности;

«Организация ЭВМ и вычислительных систем» – знать технические характеристики, показатели качества ЭВМ и систем, методы их оценки и пути совершенствования, уметь проводить анализ архитектуры и структуры ЭВМ и систем, оценивать эффективность архитектурно-технических решений, анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем, владеть методиками оценки показателей качества и эффективности ЭВМ и вычислительных систем;

«Безопасность систем баз данных» – знать средства обеспечения безопасности данных, последовательность и содержание этапов проектирования баз данных, разрабатывать и администрировать базы данных, уметь применять средства обеспечения безопасности данных, реализовывать политику безопасности баз данных, навыками эксплуатации и администрирования баз данных с учетом требований по обеспечению информационной безопасности; навыками разработки, документирования баз данных с учетом требований по обеспечению информационной безопасности;

«Электроника и схемотехника» – знать типовые схемотехнические решения основных узлов и блоков электронной аппаратуры, уметь использовать стандартные методы и средства проектирования цифровых узлов и устройств, в том числе для средств защиты информации, владеть навыками использования измерительного оборудования при экспериментальном исследовании электронной аппаратуры;

«Технологии и методы программирования» – знать современные технологии и методы программирования, методологии и методы проектирования программного обеспечения, принципы организации документирования разработки, процесса сопровождения программного обеспечения, уметь формировать требования и разрабатывать внешние спецификации для разрабатываемого программного обеспечения, планировать разработку сложного программного обеспечения, проектировать структуру и архитектуру программного обеспечения с использованием современных методологий и средств автоматизации проектирования программного обеспечения.

Дисциплина «Разработка и эксплуатация защищенных автоматизированных систем» является предшествующей для изучения базовой дисциплины «Управление информационной безопасностью», а также дисциплин вариативной части профессионального цикла, предусмотренных примерным учебным планом.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

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

способность использовать языки, системы и инструментальные средства программирования в профессиональной деятельности (ПК-3);

способность применять достижения современных информационных технологий для поиска и обработки больших объемов информации по профилю деятельности в глобальных компьютерных системах, сетях, в библиотечных фондах и в иных источниках информации (ПК-4);

способность применять методологии научно-исследовательской и практической деятельности (ПК-5).

способность использовать нормативные и правовые документы в своей профессиональной деятельности (ПК- 6);

способность к освоению новых образцов программных, технических средств и информационных технологий (ПК-8);

способность осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере своей профессиональной деятельности (ПК-9);

способность применять современные методы исследования с использованием компьютерных технологий (ПК-10);

способность разрабатывать и исследовать модели автоматизированных систем (ПК-11);

способность проводить анализ защищенности автоматизированных систем (ПК-12);

способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы (ПК-13);

способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем (ПК-15);

способность разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ (ПК-16);

способность проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем (ПК-17);

способность участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности (ПК-18);

способность проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-23);

способность проводить инструментальный мониторинг защищенности автоматизированных систем (ПК-26);

способность организовать эксплуатацию автоматизированной системы с учетом требований информационной безопасности (ПК-30);

способность разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автомати-

зированных систем, а также положений, инструкций и других организационно-распорядительных документов в сфере профессиональной деятельности (ПК-31);

способность проводить анализ особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите (ПК-32);

способность обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности (ПК-35);

способность обеспечить восстановление работоспособности систем защиты информации при возникновении нештатных ситуаций (ПК-40).

В результате изучения дисциплины студент должен

знать:

основные информационные технологии, используемые в автоматизированных системах;

основные угрозы безопасности информации и модели нарушителя в автоматизированных системах;

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

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

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

методы, способы и средства обеспечения отказоустойчивости автоматизированных систем;

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

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

уметь:

администрировать подсистемы информационной безопасности автоматизированных систем;

восстанавливать работоспособность подсистемы информационной безопасности автоматизированных систем в нештатных ситуациях;

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

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

владеть:

навыками работы с технической документацией на компоненты автоматизированных систем на русском и иностранном языках;

навыками анализа основных узлов и устройств современных автоматизированных систем;

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

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

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

навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем.

4. Содержание дисциплины

Раздел 1. Разработка защищенных автоматизированных систем

Тема 1. Защищенные АИС. Основные понятия и классификация

Тема 2. Основы организации разработки защищенных АИС

Тема 3. Общие принципы проектирования защищенных АИС

Раздел 2. Эксплуатация защищенных автоматизированных систем

Тема 4. Основы эксплуатации защищенных АИС

Тема 5. Диагностика программных и аппаратных средств АИС.

Аннотация рабочей программы дисциплины «Управление информационной безопасностью»

1. Цели и задачи дисциплины

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

Задачами дисциплины являются:

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

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

2. Место дисциплины в структуре ООП

Дисциплина "Управление информационной безопасностью" относится к числу дисциплин базовой части профессионального цикла.

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

"Правоведение" – знать основы права и законодательства России, уметь использовать в практической деятельности правовые знания, анализировать основные правовые акты, давать правовую оценку информации, используемой в профессиональной деятельности; владеть навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности;

"Основы управленческой деятельности" – знать научные основы, цели, принципы, методы и технологии управленческой деятельности; уметь работать в коллективе, принимать управленческие решения и оценивать их эффективность; владеть навыками выбора, обоснования, реализации и контроля результатов управленческого решения;

"Основы информационной безопасности" – знать сущность и понятие ИБ и характеристику ее составляющих, источники и классификацию угроз ИБ, основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; уметь классифицировать и оценивать угрозы информационной безопас-

ности для объекта информатизации; владеть профессиональной терминологией в области информационной безопасности;

"Программно-аппаратные средства обеспечения информационной безопасности" – знать программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных и компьютерных сетях; уметь проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы; владеть навыками использования программно-аппаратных средств обеспечения безопасности компьютерных сетей;

"Разработка и эксплуатация защищенных автоматизированных систем" – знать методы, способы, средства, последовательность и содержание этапов разработки подсистем безопасности АС, основные меры по защите информации в автоматизированных системах, криптографические методы, используемые для обеспечения ИБ в АС; уметь администрировать подсистемы информационной безопасности автоматизированных систем, исследовать эффективность создаваемых средств автоматизации; владеть методами и технологиями проектирования, моделирования, исследования подсистем безопасности автоматизированных систем, навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем; навыками анализа информационной инфраструктуры безопасности АС;

"Безопасность жизнедеятельности" – знать опасные и вредные факторы системы «человек – среда обитания»; уметь реализовывать и контролировать выполнение требований по охране труда и технике безопасности в профессиональной деятельности, применять основные методы защиты производственного персонала и населения от возможных последствий аварий; владеть навыками безопасного использования технических средств в профессиональной деятельности.

Дисциплина является предшествующей для прохождения практики и итоговой государственной аттестации.

3. Требования к результатам освоения дисциплины

В результате изучения дисциплины "Управление информационной безопасностью" обучающиеся должны

обладать следующими **компетенциями:**

способность применять методологии научно-исследовательской и практической деятельности (ПК-5)

способность использовать нормативные и правовые документы в своей профессиональной деятельности (ПК- 6);

способность разрабатывать и исследовать модели автоматизированных систем (ПК-11)

способность проводить анализ защищенности автоматизированных систем (ПК-12);

способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы (ПК-13);

способность проводить анализ рисков информационной безопасности автоматизированной системы (ПК-14);

способность проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем (ПК-17);

способность участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности (ПК-18);

способность разрабатывать политики информационной безопасности автоматизированных систем (ПК-20);

способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы (ПК-21);

способность организовывать работу малых коллективов исполнителей, находить и принимать управленческие решения в сфере профессиональной деятельности (ПК-27);

способность разрабатывать оперативные планы работы первичных подразделений (ПК-28);

способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы (ПК-29);

способность организовать эксплуатацию автоматизированной системы с учетом требований информационной безопасности (ПК-30);

способность разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, а также положений, инструкций и других организационно-распорядительных документов в сфере профессиональной деятельности (ПК-31);

способность проводить анализ особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите (ПК-32);

способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации (ПК-33);

способность формировать комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной системы (ПК-34);

способность администрировать подсистему информационной безопасности автоматизированной системы (ПК-37);

способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы (ПК-38);

способность управлять информационной безопасностью автоматизированной системы (ПК-39).

В результате изучения дисциплины студент должен

знать:

– основные методы управления информационной безопасностью;

– методы аттестации уровня защищенности автоматизированных систем;

– основные угрозы безопасности информации и модели нарушителя в автоматизированных системах;

– принципы формирования политики информационной безопасности в автоматизированных системах;

уметь:

– определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите;

– разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем;

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

– оценивать информационные риски в автоматизированных системах;

– определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем, составлять аналитические обзоры по вопросам обеспечения информационной безопасности автоматизированных систем;

– разрабатывать частные политики информационной безопасности информационной безопасности автоматизированных систем;

– контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем;

– разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем;

владеть:

– навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности;

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

– методами управления информационной безопасностью автоматизированных систем;

– методами оценки информационных рисков;

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

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

4. Содержание дисциплины

Тема 1. Введение

Тема 2. Система управления информационной безопасностью автоматизированных систем

Тема 3. Политика безопасности автоматизированных систем

Тема 4. Организация обеспечения информационной безопасности автоматизированных систем

Тема 5. Аудит информационной безопасности автоматизированных систем

Тема 6. Средства поддержки процессов управления информационной безопасностью АС.

Требования к выполнению выпускной квалификационной работы по специальности

090303.65 Информационная безопасность автоматизированных систем

Оглавление

1. ОБЩИЕ ПОЛОЖЕНИЯ

В соответствии с ФГОС по специальности 090303 «Информационная безопасность автоматизированных систем», выпускная квалификационная работа специалиста по защите информации (дипломная работа или дипломный проект) имеет целью систематизировать и углубить знания, совершенствовать навыки и умения выпускника в решении сложных комплексных научно-технических задач с элементами научного исследования, а также проявить степень профессиональной подготовленности выпускника, ее соответствие данному образовательному стандарту.

Дипломный проект представляет собой решение конкретной практической задачи, имеющей прикладной характер, или инженерной проблемы с проведением проектно-конструкторских расчетов и разработок, теоретических и экспериментальных исследований.

Цель дипломного проектирования

Выполнение дипломного проекта является заключительным этапом обучения студентов в ВУЗе. Дипломный проект представляет собой самостоятельную работу, целью которой является систематизация и расширение теоретических знаний и их практическое применение в процессе ее написания.

Период дипломного проектирования состоит из нескольких этапов:

- выбор и закрепление объекта преддипломной практики;
- выбор и закрепление темы дипломного проекта;
- разработка и утверждение задания на дипломный проект;
- сбор материала для дипломного проекта на объекте практики;
- защита отчета по преддипломной практике;
- написание и оформление дипломного проекта;
- предварительная защита работы на кафедре;
- внешнее рецензирование проекта;
- защита проекта на заседании Государственной аттестационной комиссии (ГАК).

Выполнение ВКР является заключительным этапом обучения. ВКР представляет собой самостоятельную работу, целью которой является систематизация и расширение теоретических знаний, и их практическое применение в процессе ее написания.

При работе над дипломным проектом студент, обучающийся по специальности «Информационная безопасность автоматизированных систем» должен:

знать:

- основные понятия защиты информации (субъекты, объекты, доступ, информационные потоки);

- угрозы безопасности информации. Понятия политики безопасности. Угрозы конфиденциальности, целостности, доступности, раскрытия параметров АС;
- Основные положения критериев безопасности. Основные положения руководящих документов ФСТЭК РФ в области защиты информации. Определение и классификация НСД. Модели нарушителя. Классы защищенности АС от НСД и информации.
- Современные методы и средства обеспечения безопасности ОС, СУБД, вычислительных сетей;
- принципы организации и функционирования СЗИ, вычислительных систем комплексов и сетей, их компоненты, характеристики, архитектуру, возможные области применения;
- методы защиты распределенных систем обработки информации, современные сетевые технические и программные средства защиты информации, модели и структуры СЗИ информационных сетей, оценки их эффективности;
- принципы организации и построения баз данных, баз знаний, экспертных систем, пути, методы и средства защиты и интеллектуализации информационных систем;
- современные методы и средства разработки СЗИАС;
- принципы, модели и методы управления безопасностью информационных систем, тенденции их развития, связь со смежными областями;

владеть:

- современными методами системного анализа угроз информационным процессам и системам, принципами, методами и средствами построения СЗИ в АС;
- математическими моделями, методами анализа, синтеза и оптимизации ИБАС;
- методами и инструментальными средствами исследования, моделирования и проектирования СЗИ распределенных, корпоративных информационно-управляющих систем;
- методами и средствами проектирования и комплексирования аппаратных и программных средств СЗИ;
- современными правовыми нормами организации разработки и эксплуатации СЗИ и их программного обеспечения;
- методами оценки эффективности СЗИ информационных систем, аудита ИБ, сертификации и аттестации СЗИАС и их компонентов.

2. ВЫБОР ТЕМЫ И НАУЧНОГО РУКОВОДИТЕЛЯ ВЫПУСКНОЙ

КВАЛИФИКАЦИОННОЙ РАБОТЫ

Согласно установленным срокам студент должен подать заявление о закреплении выбранной темы дипломного проекта и назначении руководителя и консультанта. Заявление пишется на имя директора института. При этом указанный руководитель должен поставить на заявлении свою подпись, что будет означать его согласие на руководство.

Утверждение темы, руководителя и консультанта дипломного проекта закрепляется приказом по Университету. Название темы должно состоять из двух частей: в первой части указывается суть дипломного проекта, а во второй - субъект для которого ведётся разработка. Например: «Разработка программно-технического комплекса СЗИ корпоративной АИС концерна «Вега», «Разработка предложений по выявлению уязвимостей ЛВС предприятия НПО «Агат», «Разработка защищенной автоматизированной информационной сети банка «Возрождение».

Тема дипломного проекта должна быть актуальной и иметь научно практическую направленность.

Следует обратить внимание на то, что тема дипломной работы должна быть ***абсолютно*** одинаковой во ***всех*** документах, а именно в:

- Приказе о темах дипломных проектов;
- Титульном листе дипломного проекта;
- Задании на дипломный проект;
- Направлении на ГАК;
- Отзыве руководителя дипломного проекта;
- Рецензии на дипломный проект;

Руководитель дипломного проекта осуществляет теоретическую и практическую помощь студенту в период подготовки и написания дипломного проекта, дает студенту рекомендации по структуре, содержанию и оформлению работы, подбору литературных источников и т. д. Кроме того, руководитель указывает на недостатки аргументации, композиции, стиля и т.п., советует, как их устранить.

Следует иметь в виду, что студент самостоятельно выполняет дипломный проект и оформляет всю необходимую документацию, включая демонстрационный материал, согласно требованиям специальности и указаниям руководителя. Разработка и освещение темы дипломного проекта, а также ее качество и содержание целиком и полностью лежат на ответственности студента-дипломника.

В функции консультанта входит: проверка работы на предмет (соответствия или достаточности) раскрытия темы дипломного проекта, консультирование студента по специфическим вопросам дипломного проекта: особенности оформления,

использование математических методов, особенности предметной области, особенности используемого языка программирования и т.д.

После утверждения руководителя дипломного проекта, студент совместно с ним составляют задание на дипломный проект (приложение), которое включает план работы, перечень основных литературных источников и т. д., а также формирует календарный план (приложение), Затем, в соответствии с этим заданием, студент пишет дипломный проект.

Студенту следует постоянно информировать руководителя о ходе подготовки дипломного проекта и консультироваться по вызывающим затруднение вопросам. Кроме того, студент по мере готовности должен предоставлять руководителю для прочтения части дипломного проекта, а затем готовый дипломный проект.

После прочтения окончательного варианта дипломного проекта руководитель составляет письменный отзыв, в котором характеризует качество дипломного проекта, оценивает реализацию принятых проектных решений по четырехбалльной шкале, мотивирует возможность представления дипломного проекта для предварительной защиты на кафедре.

3. СТРУКТУРА И СОДЕРЖАНИЕ ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ

Вне зависимости от решаемой задачи и подхода при проектировании структура дипломного проекта такова:

ВВЕДЕНИЕ

1. АНАЛИТИЧЕСКАЯ ЧАСТЬ
2. ПРОЕКТНАЯ ЧАСТЬ
3. ОБОСНОВАНИЕ ЭКОНОМИЧЕСКОЙ ЭФФЕКТИВНОСТИ ПРОЕКТА

ЗАКЛЮЧЕНИЕ

Список используемой литературы

Приложения

Вне зависимости от выбранной темы **ВВЕДЕНИЕ** (общим объемом не более 5 стр.) должно содержать общие сведения о проекте, его краткую характеристику, резюме. В нем необходимо отразить актуальность выбранной темы, цель и задачи, решаемые в проекте, используемые методики, практическую значимость полученных результатов. К числу задач, решаемых в дипломном проекте можно отнести:

- изучение предметной области и выявление недостатков существующей организации обработки информации, определяющих необходимость разработки

данного проекта;

- разработку постановки задачи:
- обоснование выбора основных проектных решений;
- разработку всех видов обеспечивающих подсистем;
- обоснование экономической эффективности проекта.

Дополнительно может достигаться совершенствование информационной базы, применение новых технических средств сбора, передачи, обработки и выдачи информации, математического и программного обеспечения.

Во введении необходимо также перечислить вопросы, которые будут рассмотрены в проекте, выделив вопросы, которые предполагается решить практически. Рекомендуется писать введение по завершении основных глав проекта, перед заключением. В этом случае исключена возможность несоответствия «желаемого» и «действительного».

В **ЗАКЛЮЧЕНИИ** рекомендуется определить, какие задачи были решены, определить пути их внедрения и направления дальнейшего совершенствования.

В ПРИЛОЖЕНИИ **должны быть приведены результаты выполнения контрольного примера:**

- формы первичных и результатных документов;
- распечатка на исходном языке программирования отлаженных основных расчетных модулей (около 1000 операторов языка высокого уровня);
- распечатки меню, экранных форм ввода, получаемых отчетов в разработанной системе;

Структура первой главы.

ГЛАВА ПЕРВАЯ (аналитическая)

Целью аналитической части является рассмотрение существующего состояния предметной области предприятия, организации или фирмы, характеристики их объектов или процессов, выбранных для реализации в дипломном проекте; выявление проблем и недостатков в работе систем и обоснование предложений по устранению выявленных недостатков, внедрению новых подходов, новых технологий и т.д.

Ниже рассматриваются особенности содержания первой главы дипломного проекта.

1. Технико-экономическая характеристика предметной области

1.1. Характеристика предприятия (объектов, процессов и явлений). Основные определения, понятия и терминология. Описание выбранного комплекса задач (задачи).

1.2. Анализ существующих разработок и выбор стратегии решения задач.

1.3. Постановка задачи дипломного проектирования.

1.4. Выбор и обоснование математического аппарата для решения поставленной задачи.

В первом параграфе главы необходимо выполнить обзор и анализ состояния вопросов, (задач), подлежащих разработке в проекте; ввести основные определения, понятия и терминологию.

Далее следует перечислить выделенные задачи, описать их связи с другими задачами, входящими в комплекс. В этот раздел целесообразно включить информационную модель декомпозиции и взаимосвязи комплекса задач и указать место выбранных задач в комплексе.

Второй параграф посвящен анализу имеющихся разработок по избранной теме, результатом которого должны являться предложения по совершенствованию объекта исследования. Обзор существующих разработок необходимо проводить с помощью Internet. Адреса используемых при обзоре ресурсов следует добавить в список литературы дипломного проекта. Результаты, выполненные в этом параграфе можно представить в виде схем или таблиц.

В третьем параграфе необходимо сформулировать задачу разработки дипломного проекта. Цель решения задачи должна сводиться к устранению тех недостатков, которые были отличены в предыдущем параграфе главы. При описании назначения решения задачи дипломанту следует сделать акцент на требования к будущему проекту (функциональные требования, требования к надежности, техническим характеристикам, совместимости и т.д.). Постановка задачи может быть выполнена на содержательном уровне и в виде математической модели.

В четвертом параграфе первой главы необходимо выбрать и обосновать необходимость применения математического аппарата для решения поставленной задачи. В разделе описываются выбранные математические методы и модели, причем их можно использовать в нескольких направлениях, например: для решения оптимизационных экономических задач при математической обработке результатов исследований, при оценке разработанного программного технического комплекса и т.д.

При использовании достаточно обширного материала возможно изложение его в отдельной главе.

Результаты работы над дипломным проектом по первой главе необходимо представить в качестве презентационного материала при выступлении на защите.

Структура второй главы

ГЛАВА ВТОРАЯ (проектная)

Вторая (проектная) часть дипломного проекта является описанием решений, принятых в первой главе и должна быть основана на информации, представленной в

аналитической части, обобщать ее. Вторая глава посвящена разработке конкретных предложений по совершенствованию объекта исследования.

Содержание второй главы дипломного проекта:

2. Разработка математической модели решения поставленной задачи.

2.1. Обоснование выбора математического аппарата.

2.3. Разработка математической модели.

2.4. Обоснование полученных результатов исследования.

Во второй главе необходимо выполнить следующее:

1) выбрать и обосновать количественные показатели, посредством которых можно произвести оценку достигнутого уровня совершенства предмета исследования;

2) описать исходную информацию, обсудить степень ее достоверности и возможности использования для получения количественных оценок показателей;

3) выбрать критерии, позволяющие на основе количественных показателей принимать решения в пользу того или иного варианта (направления) совершенствования предмета исследования;

4) обсудить обоснованность выбранных критериев;

5) по возможности с использованием выбранных критериев формализовать поставленные задачи (в лучшем случае произвести математическую постановку задачи);

6) описать исходную информацию для решения поставленных задач.

7) осуществить разработку (или обосновать выбор) модели, посредством которой может быть описан предмет (объект) исследования. Модель может быть математической, имитационной и т.д., но любая модель должна позволять произвести количественные оценки выбранных показателей в различных условиях обстановки.

В этой же главе следует сделать все необходимые расчеты, построить необходимые графические зависимости количественных показателей от параметров, характеризующих предмет исследования и окружающую среду.

Структура третьей главы

ГЛАВА ТРЕТЬЯ

Содержит экспериментальную проверку и оценку разработанных предложений (например, архитектуры программно-технического средства).

Ниже рассматриваются особенности содержания третьей главы дипломного проекта.

3. Экспериментальная проверка и оценка разработанного программно-технического комплекса.

3.1 Описание результатов вычислительного эксперимента.

3.2 Оценивание характеристик качества разработанного программно-

технического комплекса.

3.3 Обоснование экономической эффективности проекта.

В третьей главе необходимо на основании полученных количественных оценок, используя параметры реального объекта, проанализировать целесообразность его совершенствования в выбранном направлении и разработать предложения, практические рекомендации применительно к реальному объекту.

При этом качестве критериев могут быть использованы простые сравнения типа "лучше, потому что дешевле", или "потому что быстрее", или "дороже, но быстрее" и т.п. Эти сравнения должны быть подтверждены количественными оценками. Более полное и обоснованное решение в пользу того или иного варианта совершенствования предмета исследования и предложений по реальному объекту могут быть сделаны посредством решения задачи оптимизации с использованием критериев минимума затрат, максимума эффективности и т.д.

В этой же главе следует произвести оценку эффекта, получаемого от совершенствования предмета (объекта) исследования, от практических предложений, формулируемых дипломником по результатам исследований.

В завершении третьей главы необходимо описать конкретные пути реализации сформулированных предложений, сводящихся к изменениям либо в функционировании системы (элемента системы), ее внутренней структуре, либо в организации и построении процессов, имеющих место в системе, либо в документации, обеспечивающей функционирование системы и организацию процессов.

4. ОБЩИЕ ТРЕБОВАНИЯ К ОФОРМЛЕНИЮ ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ

Текстовый материал работы должен быть представлен в машинописном варианте с использованием текстового редактора. При оформлении дипломного проекта в текстовом редакторе следует соблюдать следующие параметры: выбранный шрифт должен быть четким и разборчивым (рекомендуется «Times New Roman»), размер шрифта-14, печать через 1.5 интервала.

Названия глав, параграфов, пунктов, подпунктов следует начинать с абзаца, их можно писать более крупным кеглем, чем текст. Допускается выделение интенсивностью (полужирный шрифт).

Основной объем работы должен составлять 70-90 страниц. Объем приложения не ограничен. Текст наносится только с одной стороны листа формата А4, при этом следует соблюдать следующие отступы: слева - 3 см., справа - 1 см., сверху- 2 см., снизу – 2 см.

Каждая глава должна начинаться с новой страницы. Все страницы работы должны быть пронумерованы последовательно арабскими цифрами. Номер должен располагаться в середине страницы в 1-2 мм от ее верхнего края. Нумерация страниц должна быть сквозной от титульного листа до последнего листа текста, включая иллюстративный материал (таблицы, графики, диаграммы и т.п.), расположенный внутри текста или после него, а также приложения. На титульном листе, который является первой страницей, а также задании на дипломный проект и странице, содержащей оглавление, номера страниц не ставятся, но учитываются при общей нумерации. Нумерация страниц должна соответствовать оглавлению (содержанию).

Сокращения в тексте не допускаются. Исключения составляют:

- общепринятые сокращения мер веса, длины и т.д.;
- те сокращения, для которых в тексте приведена полная расшифровка.

Расшифровка сокращения должна предшествовать самому сокращению. Сокращение, встречающееся в тексте в первый раз указывается в скобках, сразу за его расшифровкой. Например: ... орган Государственной Налоговой Инспекции (ГНИ) ... Далее по тексту сокращение употребляется уже без скобок. Используемые сокращения или аббревиатуры рекомендуется выделить в «Список сокращений», размещаемый после Заключения.

Специфические понятия и термины, используемые в тексте дипломного проекта, рекомендуется оформить в виде отдельного «Глоссария», содержащего толкование данных понятий. Глоссарий размещается аналогично списку сокращений.

При написании в тексте формул значения символов и числовых коэффициентов должны быть приведены непосредственно под формулой, с новой строки в той же последовательности, в какой они приведены в формуле. Первая строка расшифровки начинается словом «где» без двоеточия после него. Если в тексте есть ссылки на формулы, то формулам необходимо присвоить порядковые номера, которые проставляются на уровне формулы арабскими цифрами в круглых скобках. Причем первый знак означает номер главы, а последующие - номер формулы в пределах главы.

Например: «.в формуле (1.3)».

При написании формул, не помещающихся по ширине печатного листа, их разделяют на несколько строк. Перенос допускается только на знаках равенства, сложения, вычитания, деления и умножения. При переносе вышеуказанные знаки повторяются в начале и в конце строк.

При приведении цифрового материала должны использоваться только арабские цифры, за исключением общепринятой нумерации кварталов, полугодий и т.д., которые обозначаются римскими цифрами. Количественные числительные, римские цифры, а также даты, обозначаемые арабскими цифрами, не должны сопровождаться

падежными окончаниями.

Математические знаки, такие как «+», «-», «<», «>» «=» и т.д., используются только в формулах. В тексте следует писать словами: плюс, минус и т.д. Знаки «№», «§», «%» применяются только вместе с цифрами. В тексте употребляются слова: «номер», «параграф», «процент».

Если в тексте необходимо привести ряд величин одной и той же размерности, то единица измерения указывается только после последнего числа. Для величин, имеющих два предела, единица измерения пишется только один раз при второй цифре.

На дипломный проект студент должен оформить и представить дискету с текстом дипломного проекта, презентацией и файлом- паспортом.

В файле-паспорте должны содержаться следующие данные:

- фамилия, имя, отчество;
- полное название специальности;
- группа;
- дата защиты и номер ГАК;
- тема дипломного проекта по приказу;
- фамилия и инициалы руководителя;
- организация руководителя;
- фамилия и инициалы консультанта;
- организация консультанта;
- фамилия и инициалы рецензента;
- организация рецензента;
- телефон студента;
- электронный адрес студента.

Наименование файла-паспорта должно быть фамилию студента, год выпуска, номер группы и символ «п». Файл должен быть представлен в формате MS Word. Например, для студента Новикова наименование файла будет выглядеть следующим образом: «п-Новиков-2005-ДКБ501Лос».

Дипломный проект может быть представлен в виде одного или нескольких файлов. В первом случае наименование файла, содержащего дипломный проект, формируется аналогично файлу-паспорту, с той лишь разницей, что вместо символа «п» добавляется символ «д». Если дипломный проект состоит из нескольких файлов, то все они должны быть пронумерованы.

Правила оформления иллюстративного материала

Необходимым условием оформления дипломного проекта является иллюстративный материал, который может быть представлен в виде рисунков, схем, таблиц, графиков, диаграмм. Иллюстрации должны наглядно дополнять и

подтверждать содержание текстового материала и отражать тему дипломного проекта. На каждую единицу иллюстративного материала должна быть хотя бы одна ссылка в тексте дипломного проекта.

В том случае, когда текст иллюстрируется таблицами, они оформляются следующим образом. Таблицы рекомендуется размещать сразу после ссылки на них в тексте. Таблицы могут нумероваться последовательно арабскими цифрами в пределах всей работы или главы. Над правым верхним углом таблицы помещают надпись «Таблица №». Ниже, посередине страницы обязательно должен быть помещен тематический заголовок таблицы.

При большом размере таблицы следует переносить ее шапку на каждую последующую страницу. Тематический заголовок таблицы переносить не следует, однако над ее правым верхним углом необходимо указывать номер таблицы после слова «Продолжение». Пример: «Продолжение таблицы №».

Все иллюстрации, не относящиеся к таблицам (схемы, графики, диаграммы и т.д.), именуются рисунками. Им присваивается последовательная нумерация либо по всему текста, либо в пределах главы. Все рисунки должны иметь полные наименования и ссылки на них в тексте. Номер и наименование рисунка записываются в строчку под его изображением посередине страницы. Например: «Рис.3.1. Блок-схема основного модуля».

При продолжении рисунка на следующей странице его наименование указывать не следует, однако под рисунком необходимо указывать его номер после слова «Продолжение». Например: «Продолжение Рис. №».

Следует обратить внимание, что слова «Таблица» и «Рисунок» начинаются с большой буквы. Ссылки на иллюстративный материал в тексте дипломного проекта могут начинаться с маленькой буквы. Номера таблиц и рисунков указываются без каких-либо дополнительных символов.

Правила составления списка литературы

Использованные в процессе работы специальные литературные источники указываются в конце дипломного проекта перед приложением. Список использованной литературы входит в основной объем работы. На каждый литературный источник в тексте работы обязательно должна быть хотя бы одна ссылка.

Список литературы должен быть составлен в алфавитном порядке, т.к. в этом случае легче указывать ссылки на литературу в тексте дипломного проекта.

При составлении списка литературы в алфавитном порядке следует придерживаться следующих правил и их расположения:

1) законодательные акты и постановления правительства РФ;
2) специальная научная литература;

3) методические, справочные и нормативные материалы, статьи периодической печати;

4) названия и адреса Интернет-ресурсов.

Для многотиражной литературы при составлении списка указываются: полное название источника, фамилия и инициалы автора, издательство и год выпуска (для статьи - название издания и его номер).

Для законодательных актов необходимо указывать их полное название, принявший орган и дату принятия.

При использовании Интернет-ресурсов сначала приводится название материала и автор (если указан), а затем полный адрес его размещения (включая страницу). Ссылка должны быть актуальна на момент защиты проекта. В случае потери ссылкой актуальности - указать дату, на которую ссылка была рабочей.

Пример списка литературы:

1. Безопасность операционных систем: Учебник / Под ред. проф. А.Б. Иванова - Москва: Финансы и Статистика, 2006. - 272 стр.: ил..
2. Тельнов Ю.Ф. Реинжиниринг бизнес-процессов, Москва.: Финансы и Статистика, 2009. - 256 стр.
3. Приказ от 26.12.94 № 170 О положении о бухгалтерском учете и отчетности в Российской Федерации, приказ Минфина РФ № 170 от 26.12.10.
4. Управлениезнаниями. Введение в тему. www.knowledgemanagement.report.ru/_5FolderID_220_. html

При ссылке на литературу в тексте приводится порядковый номер источника, заключенный в квадратные скобки. При приведении дословной цитаты из источника указывается также страница, на которой содержится данная цитата. Например: «Программное обеспечение - это совокупность программ системы обработки данных и программных документов, необходимых для эксплуатации этих программ» [7].

Правила оформления приложений

Приложения оформляются как продолжение дипломного проекта на последующих ее страницах, но в основной листаж не включаются. Содержание приложений определяется студентом-дипломником по согласованию с научным руководителем. При этом в основном тексте работы целесообразно оставить только тот иллюстративный материал, который позволяет непосредственно раскрыть содержание излагаемой темы. Вспомогательный же материал выносится в приложения. Объем приложений не ограничивается, поэтому основной листаж можно регулировать за счет переноса иллюстративного материала в приложения или из приложений.

Если приложения однородны по своему составу, то им предшествует отдельный лист с надписью «Приложение». В том случае, когда в работе содержатся приложения

нескольких видов, они нумеруются последовательно арабскими цифрами: «Приложение 1», «Приложение 2» и т.д., кроме того каждое приложение может иметь свое тематическое название. Например: Приложение 5. Текст основных программных модулей. На каждое приложение в тексте работы обязательно должна быть хотя бы одна ссылка.

5. ПРЕДЗАЩИТА ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ

Предварительная защита дипломного проекта происходит на выпускающей кафедре. Дни и время предварительной защиты вывешиваются на стенде соответствующей кафедры в середине мая. Предварительная защита происходит перед комиссией, в которую входят заведующий кафедрой и преподаватели кафедры.

- Для предварительной защиты студенту необходимо иметь
- готовый дипломный проект и направление в ГАК,
- подписанный отзыв научного руководителя,
- презентацию,
- комплект графических материалов.

В процессе предварительной защиты студент кратко излагает суть дипломного проекта и отвечает на вопросы членов комиссии. После ознакомления с дипломным проектом и получения ответов студента, комиссия принимает решение о возможности его защиты в ГАК. В случае принятия положительного решения проект представляется для рецензирования.

6. РЕЦЕНЗИРОВАНИЕ ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ

Рецензирование дипломного проекта проводится с целью получения дополнительной объективной оценки труда студента от специалистов в соответствующей области.

Состав рецензентов утверждается директором института. В качестве рецензентов могут привлекаться специалисты государственных органов, сферы бизнеса, производства, НИИ, а также профессора и преподаватели других вузов.

В рецензии должно быть отмечено значение изучения данной темы, ее актуальность, теоретическая и практическая ценность, а также насколько успешно студент справился с раскрытием темы работы и рассмотрением теоретических и практических вопросов. Затем дается развернутая характеристика каждого раздела дипломного проекта с выделением положительных сторон и недостатков. В заключении рецензент излагает свою точку зрения об общем уровне дипломного проекта, оценивает ее по четырехбалльной шкале и делает вывод о возможности защиты дипломного проекта в ГАК. Объем рецензии должен составлять 2-3 страницы

печатного текста.

При получении студентом рецензии ему, совместно с руководителем дипломного проекта, следует подготовить ответ на замечания рецензента и, в случае необходимости, внести соответствующие доработки и исправления в дипломный проект. В случае выявления рецензентом серьезных недостатков в дипломной работе, после их устранения, выпускающая кафедра вправе отправить проект на повторное рецензирование. В случае, если заведующий кафедрой на основании содержания отзывов руководителя, и/или результатов предварительной защиты и/или замечаний рецензента не считает возможным допустить студента к защите дипломного проекта в ГАК, этот вопрос решается на заседании кафедры с участием студента и руководителя дипломного проекта.

7. ПОДГОТОВКА К ЗАЩИТЕ ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ

При оформлении документации по дипломному проектированию необходимо подготовить для представления в ГАК следующие документы:

1. Дипломный проект (включающий сам дипломный проект, ТЗ);
2. Отзыв руководителя;
3. Рецензию на дипломный проект;
4. Графический материал (не менее шести листов);
5. Презентацию.

За три дня до назначенной даты защиты дипломный проекта студент- дипломник должен представить всю документацию по проекту, в противном случае он будет снят с защиты в ГАК. Все документы должны содержать все необходимые подписи.

Дипломный проект обязательно должен быть переплетен в твердый переплет или сброшюрован в специальной папке. Для защиты дипломной работы необходимо подготовить демонстрационный материал, основанный на иллюстративном материале дипломной работы. Перечень иллюстраций, представляемых на защиту, определяется студентом совместно с руководителем дипломной работы.

При защите дипломного проекта иллюстративный материал оформляется на листах формата А1. Все чертежи должны содержать штамп определённой формы. Образец штампа представлен в приложении 1. Штамп помещается в правом нижнем углу листа внутри рамки. Отступы для рамки: слева - 2см, справа - 0,5см, сверху - 0,5см, снизу - 0,5 см. Никакие заголовочные надписи на чертежах не разрешаются.

К этим листам могут относится:

- информационная модель/ ER-модель/ диаграмма потоков данных;
- схема технологического процесса решения задачи или схема работы системы;
- результаты расчёта надежности и экономической эффективности

программного обеспечения проекта (графики и итоговая таблица);

- организационная структура предприятия / схема документооборота предприятия / управленческая структура предприятия;
- схема архитектуры информационной системы предприятия;
- описание математических моделей, алгоритмов и методов;
- схема архитектуры и структуры программного обеспечения;
- и другие схемы, отражающие проектные решения и представленные в дипломной проекте.

Весь материал, выносимый на чертежи, слайды или в буклеты, обязательно должен быть идентичен иллюстрациям, представленным в дипломном проекте.

Рекомендуемые темы выпускной квалификационной работы

№ п/п	Тема выпускной квалификационной работы
1	Разработка концепции информационной безопасности конкретной организации (коммерческого банка, предприятия торговли, промышленного предприятия)
2	Разработка рекомендаций по поиску и нейтрализации средств несанкционированного съема информации на объектах информатизации (конкретный объект)
3	Разработка фрагментов программно-аппаратного комплекса, реализующего задачи обеспечения защиты персональных данных организации
4	Обеспечение безопасности баз данных информационно-аналитических подразделений организации (на примере федеральных органов налоговой полиции, и др)
5	Применение методов аналитической разведки при решении задач стратегического планирования
6	Разработка ситуационных методов оценки деятельности конкурентов в условиях вялотекущего кризиса
7	Разработка предложений по применению криптографических методов защиты информации в системах электронного документооборота
8	Разработка предложений по созданию и внедрению автоматизированной защищенной системы кадрового резерва организации
9	Разработка методологии обеспечения информационной безопасности виртуальных интернет - организаций
10	Обеспечение защиты информации компании при попытке её захвата рейдерами
11	Разработка защищенного интернет - сайта организации
12	Разработка модели пространства информационных помех, воздействующих на принятие управленческих решений
13	Изучение влияния уровня развития технических средств несанкционированного съема информации на разработку политики безопасности
14	Исследование теоретических вопросов обеспечения информационной безопасности (на примере конкретной задачи)
15	Оценка возможностей использования информационно-аналитических систем для получения сведений из зоны "невидимого Интернета" при решении практических задач аналитической разведки
16	Разработка предложений по проведению аудита информационной безопасности образовательного учреждения
17	Методы защиты информационных ресурсов ВУЗа, реализуемые при проведении дистанционного образования