МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ
ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ им. В.Г.ШУХОВА»
(БГТУ им. В.Г.Шухова)

Утверждаю:
Ректор БГТУ им. В.Г. Шухова
д-р экон. наук, профессор
_____ С.Н. Глаголев
«29» ____01____ 2017 г.

Основная образовательная программа
высшего образования

Направление подготовки
10.05.03 «Информационная безопасность автоматизированных систем»

Специализация
«Обеспечение информационной безопасности
распределенных информационных систем»

Квалификация

Специалист по защите информации

Форма обучения - очная

Белгород 2017

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Образовательная программа (ОП) специалитета, реализуемая государственным образовательным учреждением высшего образования «Белгородский государственный технологический университет им. В.Г. Шухова» по направлению подготовки 10.05.03 «Информационная безопасность автоматизированных систем» и профилю подготовки «Обеспечение информационной безопасности распределенных информационных систем» представляет собой систему документов, разработанную и утвержденную высшим учебным заведением с учетом требований рынка труда на основе Федерального государственного образовательного стандарта по соответствующему направлению подготовки высшего образования (ФГОС ВО), а также с учетом рекомендованной примерной основной образовательной программы.

1.2. Нормативные документы для разработки ОП специалитета по направлению подготовки «Информационная безопасность автоматизированных систем»

Нормативную правовую базу разработки ОП специалитета составляют:

- Федеральный закон от 29 декабря 2012 года №273-ФЗ «Об образовании в Российской Федерации»;
- Порядок разработки примерных основных образовательных программ, проведения их экспертизы и ведения реестра примерных основных образовательных программ, утверждённый приказом Минобрнауки России от 28 мая 2014 года № 594;
- Федеральный государственный образовательный стандарт высшего профессионального образования (ФГОС ВО) по направлению подготовки специалитета 10.05.03 «Информационная безопасность автоматизированных систем», утвержденный приказом Министерства образования и науки Российской Федерации от «01» декабря 2016г. №1509;
- Порядок организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам магистратуры, программам специалитета, утверждённый приказом Минобрнауки России от 13 декабря 2013 года №1367 (далее – Порядок организации образовательной деятельности);
- Порядок проведения государственной итоговой аттестации по образовательным программам высшего образования – программам бакалавриата, программам специалитета и программам магистратуры, утверждённый приказом Минобрнауки России от 29 июня 2015 г. № 636;
- Положение о практике обучающихся, осваивающих основные профессиональные образовательные программы высшего образования, утверждённое приказом Минобрнауки России от 27 ноября 2015 г. № 1383.
- Устав университета.

1.3. Общая характеристика основной образовательной программы высшего профессионального образования

1.3.1. Цели и задачи ООП ВО специалитета по направлению подготовки 10.05.03 «Информационная безопасность автоматизированных систем»

Целью разработки ООП ВО по направлению подготовки 10.05.03 «Информационная безопасность автоматизированных систем» является научно - методическое обеспечение реализации в БГТУ им. В.Г. Шухова ФГОС ВО подготовки специалиста по направлению «Информационная безопасность автоматизированных систем».

В ходе реализации ОП у студентов формируются общекультурные (универсальные, общенаучные, социально - личностные, инструментальные) и профессиональные компетенции в соответствии с требованиями ФГОС ВО по направлению подготовки 10.05.03 «Информационная безопасность автоматизированных систем», а также развитие личностных качеств (целеустремленности, организованности, трудолюбия, ответственности, гражданственности, коммуникативности, толерантности, общей культуры), позволяющих реализовать сформированные компетенции в профессиональной деятельности.

Основными задачами ОП являются следующие:

- систематизация гуманитарных, социальных, экономических, математических, естественнонаучных и профессиональных знаний в области промышленного производства программного обеспечения в системах безопасности в рамках компетентностной модели подготовки;
- гармоничное сочетание дисциплин специализации с общей структурой профессиональной подготовки, способствующее углублению профессиональных компетенций с учетом профиля подготовки;
- обеспечение кадрового состава, материально - технических условий, нормативных, методических и других средств для реализации образовательного процесса по специальности.

1.3.2. Срок освоения ОП специалитета

Срок освоения ОП специалитета по направлению подготовки 10.05.03 «Информационная безопасность автоматизированных систем» при очной форме обучения в соответствии с ФГОС ВО по данному направлению составляет 5 лет.

1.3.3. Трудоемкость ОП специалитета по направлению 10.05.03 «Информационная безопасность автоматизированных систем»

Трудоемкость освоения студентом данной ОП за весь период обучения, включающий все виды аудиторной и самостоятельной работы студента, практики и время, отводимое на контроль качества освоения студентом ОП, составляет 300 зачетных единиц.

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 СПЕЦИАЛИТЕТА ПО НАПРАВЛЕНИЮ ПОДГОТОВКИ 10.05.03 «Информационная безопасность автоматизированных систем»

2.1. Область профессиональной деятельности выпускника

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

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

Специалист по направлению подготовки 10.05.03.-07 «Информационная безопасность автоматизированных систем» готовится к следующим видам профессиональной деятельности:

научно-исследовательская;
проектно - конструкторская;
контрольно - аналитическая;
организационно - управленческая;
эксплуатационная.

При разработке и реализации программ специалитета организация ориентируется на все виды профессиональной деятельности, к которым готовится специалист.

По окончании обучения по направлению подготовки (специальности) **10.05.03 Информационная безопасность автоматизированных систем,** присваивается квалификация «специалист по защите информации».

2.4. Задачи профессиональной деятельности выпускника

Специалист по направлению подготовки (специальности) **10.05.03 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 по проблематике информационной безопасности автоматизированных систем;

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

моделирование и исследование свойств защищенных автоматизированных систем;

анализ защищенности информации в автоматизированных системах и безопасности реализуемых информационных технологий;

разработка эффективных решений по обеспечению информационной безопасности автоматизированных систем;

проектно-конструкторская деятельность:

сбор и анализ исходных данных для проектирования защищенных автоматизированных систем;

разработка политик информационной безопасности автоматизированных систем;

разработка защищенных автоматизированных систем в сфере 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 систем управления информационной безопасностью автоматизированных систем;

контрольно-аналитическая:

контроль работоспособности и эффективности применяемых средств защиты информации;

выполнение экспериментально-исследовательские работ при сертификации средств защиты информации и аттестации автоматизированных систем;

проведение инструментального мониторинга защищенности автоматизированных систем и анализа его результатов;

организационно-управленческая деятельность:

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

организационно-методическое обеспечение обеспечения 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.

В соответствии со специализацией «Обеспечение информационной безопасности распределенных информационных систем»:

разработка и исследование моделей информационно-технологических ресурсов, модели угроз и модели нарушителей информационной безопасности в распределенных информационных системах;

удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах;

аудит защищенности информационно-технологических ресурсов;

координация деятельность подразделений и специалистов по защите информации на предприятии, в учреждении, организации.

3. КОМПЕТЕНЦИИ ВЫПУСКНИКА КАК СОВОКУПНЫЙ ОЖИДАЕМЫЙ РЕЗУЛЬТАТ ОБРАЗОВАНИЯ ПО ЗАВЕРШЕНИИ ОСВОЕНИЯ ООП ВО.

Выпускник должен обладать следующими **общекультурными компетенциями:**

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

способностью использовать основы экономических знаний в различных сферах деятельности (ОК-2);

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

способностью использовать основы правовых знаний в различных сферах деятельности (ОК-4);

способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики (ОК-5);

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

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

способностью к самоорганизации и самообразованию (ОК-8);

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

Выпускник должен обладать следующими **общепрофессиональными компетенциями**:

способностью анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач (ОПК-1);

способностью корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники (ОПК-2);

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

способностью понимать значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах (ОПК-4);

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

способностью применять нормативные правовые акты в профессиональной деятельности (ОПК-6)

способностью применять приемы первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций (ОПК-7);

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

Выпускник должен обладать следующими **профессиональными компетенциями**:

научно-исследовательская деятельность:

способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке (ПК-1);

способностью создавать и исследовать модели автоматизированных систем (ПК-2);

способностью проводить анализ защищенности автоматизированных систем (ПК-3);

способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы (ПК-4);

способностью проводить анализ рисков информационной безопасности автоматизированной системы (ПК-5);

способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности(ПК-6);

способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ (ПК-7);

проектно-конструкторская деятельность:

способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем (ПК-8);

способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности (ПК-9);

способностью применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности (ПК-10);

способностью разрабатывать политику информационной безопасности

автоматизированной системы (ПК-11);

способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы (ПК-12);

способностью участвовать в проектировании средств защиты информации автоматизированной системы (ПК-13);

контрольно-аналитическая деятельность:

способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-14);

способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информацииавтоматизированных систем (ПК-15);

способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных требований по защите информации (ПК-16);

способностью проводить инструментальный мониторинг защищенности информации в автоматизированнойсистеме и выявлять каналы утечки информации (ПК-17);

организационно-управленческая деятельность:

способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности (ПК-18);

способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы (ПК-19);

способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности (ПК-20);

способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем (ПК-21);

способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации (ПК-22);

способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа (ПК-23);

эксплуатационная деятельность:

способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности (ПК-24);

способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций (ПК-25);

способностью администрировать подсистему информационной безопасности автоматизированной системы (ПК-26);

способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы (ПК-27);

способностью управлять информационной безопасностью автоматизированной системы (ПК-28).

Выпускник должен обладать профессионально-специализированными компетенциями, соответствующими специализации № 7 «Обеспечение информационной безопасности распределенных информационных систем»:

способностью разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах (ПСК-7.1);

способностью проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах (ПСК-7.2);

способностью проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем (ПСК-7.3);

способностью проводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах (ПСК-7.4);

способностью координировать деятельность подразделений и специалистов по защите информации на предприятии, в учреждении, организации (ПСК-7.5).

Ниже представлена компетентностно-ориентированная модель подготовки по специальности 10.05.03 «Информационная безопасность автоматизированных систем».

Компетенция	Знать	Уметь	Владеть
Общекультурные компетенции (ОК)			
Способность использовать основы философских знаний для формирования мировоззренческой позиции (ОК-1)	- основные разделы и направления философии; - методы и приемы философского анализа проблем.	-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.	-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.
Способность использовать основы экономических знаний в различных сферах деятельности (ОК-2)	-основные экономические категории и закономерности; - методы анализа экономических явлений и процессов; - специфические черты функционирования хозяйственной системы на микро- и макроуровнях; - основные понятия экономической и финансовой деятельности отрасли и ее структурных подразделений.	-оценивать эффективность управленческих решений и анализировать экономические показатели деятельности подразделения.	- навыками выбора, обоснования, реализации и контроля результатов управленческого решения; – навыками работы с нормативными правовыми актами;
Способность анализировать основные этапы и закономерности исторического развития России, еѐ место и роль в современном мире для	- основные закономерности исторического процесса; - этапы исторического развития России, место и роль России в истории человечества и в современном мире; - ключевые события истории России и мира с древности до наших дней, выдающихся	- соотносить общие исторические процессы и отдельные факты, выявлять существенные черты исторических процессов, явлений и событий; - извлекать уроки из исторических событий и на их	- представлениями о событиях российской и всемирной истории, основанными на принципе историзма; - навыками анализа исторических источников; - приемами ведения

формирования гражданской позиции и развития патриотизма (ОК-3) -	деятелей отечественной истории; - различные оценки и периодизации Отечественной истории.	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.	дискуссии и полемики.
Способность использовать основы правовых знаний в различных сферах деятельности (ОК-4)	- 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.	- использовать в практической деятельности правовые знания; - анализировать и составлять правовые акты и осуществлять правовую оценку информации, используемой в профессиональной деятельности; - предпринимать необходимые меры по восстановлению нарушенных прав.	- навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности.
Способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной	- цели, задачи, принципы и основные направления обеспечения информационной безопасности; - основные термины по проблематике информационной безопасности; - роль и место информационной безопасности в системе национальной безопасности страны; - угрозы информационной безопасности государства;	- пользоваться современнойнаучно-техническойинформацией по исследуемым проблемам и задачам.	– навыками организации и обеспечения режима секретности; – методами организации и управления деятельностью служб защиты информации на предприятии; - методами формирования требований по защите информации;

деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики (ОК-5)	- содержание информационной войны, методы и средства ее ведения.		
Способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия (ОК-6)	-основные закономерности исторического процесса, этапы исторического развития России, место и роль России в истории человечества и в современном мире; – основы социологии, структуру общества и социальных институтов;	– использовать принципы, законы и методы гуманитарных, социальных и экономических наук для решения профессиональных задач; – анализировать современные общественные процессы, опираясь на принципы историзма и научной объективности;	- основными методами научного познания;
Способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной	– лексический и грамматический минимум в объеме, необходимом для работы с текстами профессиональной направленности и осуществления коммуникации на иностранном языке; – содержание и взаимосвязь основных принципов, законов, понятий и категорий гуманитарных, социальных и экономических наук;	– читать и переводить научно-техническую литературу на иностранном языке по профессиональной тематике, правильно употреблять терминологическую лексику в профессиональной речи; – использовать принципы, законы и методы гуманитарных, социальных и экономических наук для решения профессиональных задач; – анализировать современные общественные процессы, опираясь на	– навыками работы с технической документацией на компоненты автоматизированных систем на русском и иностранном языках; – иностранным языком в объёме, необходимом для получения и изложения информации по профессиональной тематике, навыками общения на иностранном языке;

деятельности (ОК-7)		принципы историзма и научной объективности; – осуществлять сбор, обработку, анализ и систематизацию научно-технической информации в области ЭВМ и систем с применением современных информационных технологий; – выделять сущности и связи предметной области; – отображать предметную область на конкретную модель данных;	– навыками письменного аргументированного изложения собственной точки зрения; – навыками публичной речи, аргументации, ведения дискуссии и полемики;
Способность к самоорганизации и самообразованию (ОК-8)	– 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 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); – 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	– анализировать мировоззренческие, социально и личностно значимые философские проблемы; – выделять сущности и связи предметной области; – отображать предметную область на конкретную модель данных;	– навыками построения дискретных моделей при решении профессиональных задач; – навыками пользования библиотеками прикладных программ для решения прикладных математических задач; методами теоретического исследования физических явлений и процессов;

	(применительно к отрасли обеспечения информационной безопасности); – общие принципы построения и использования современных языков программирования высокого уровня; – методологии и методы проектирования программного обеспечения; – сущность и понятие информации, информационной безопасности и характеристику ее составляющих;		
способность использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности (ОК-9)	- влияние оздоровительных систем физического воспитания на укрепление здоровья, профилактику профессиональных заболеваний вредных привычек; - способы контроля и оценки физического развития и физической подготовленности; - правила и способы планирования индивидуальных занятий различной целевой направленности;	- выполнять простейшие приемы самомассажа и релаксации; -выполнять приёмы защиты и самообороны, страховки и самостраховки; -осуществлять творческое сотрудничество в коллективных формах занятий физической культурой;	- навыками выбора методов физического воспитания и укрепления здоровья;
Общепрофессиональные компетенции (ОПК)			
способность анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных	- основные законы механики; основные законы термодинамики и молекулярной физики; основные законы электричества и магнетизма; - основы теории колебаний и волн, оптики; основы квантовой физики и физики твердого тела; - физические явления и эффекты, используемые при обработке, хранении, передаче, уничтожении и защите информации;	- 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; - основы физической защиты	- методами теоретического исследования физических явлений и процессов; - навыками проведения физического эксперимента и обработки его результатов навыками имитационного моделирования навыками использования

задач (ОПК-1)	- методы анализа и синтеза электронных схем.	объектов информатизации; - применять на практике методы анализа электрических цепей; - использовать стандартные методы и средства проектирования цифровых узлов и устройств, в том числе для средств защиты информации	современной измерительной аппаратуры при экспериментальном исследовании электронной аппаратуры; - навыками работы с программными средствами схемотехнического моделирования
в том числе с использованием вычислительной техники (ОПК-2)	- основы линейной алгебры над произвольными полями, векторные пространства над полями и их свойства 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; - основные понятия математической логики и теории алгоритмов; - язык и средства современной математической логики, представления	- метрические 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; - 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	- 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; - навыками использования языка современной символической логики; - навыками применения методов и фактов теории алгоритмов, относящимися к

	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; - основные понятия и методы теории вероятностей, теории случайных процессов и математической статистики; - 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; - основные понятия теории информации: энтропия, взаимная информация, источники сообщений, каналы связи, коды; основные	задач; - решать оптимизационные задачи на графах; - 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; - 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; - применять стандартные методы и модели к решению типовых теоретико-	решению переборных задач; - навыками упрощения формул алгебры высказываний и алгебры предикатов; - навыками использования стандартных теоретико-вероятностных и статистических методов при решении прикладных задач; - 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; - основами построения математических моделей систем передачи информации;

	теоремы о кодировании при наличии и отсутствии шума; - основные методы оптимального кодирования источников информации и помехоустойчивого кодирования каналов связи; - основные задачи и понятия криптографии; частотные характеристики открытых текстов и способы их применения к анализу простейших шифров замены и перестановки	вероятностных и статистических задач; - пользоваться расчетными формулами, таблицами, компьютерными программами при решении математических задач; - 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 на вычисление пределов функций, дифференцирование и интегрирование, на разложение функций в ряды; - вычислять теоретико-информационные характеристики источников сообщений и каналов связи (энтропия, взаимная информации, пропускная способность); - решать типовые задачи кодирования и декодирования;	

		работать с научно-технической литературой по тематике дисциплины	
способность применять языки, системы и инструментальные средства программирования в профессиональной деятельности (ОПК-3)	- показатели качества программного обеспечения язык программирования высокого уровня (объектно-ориентированное программирование); - возможности, классификацию и область применения макрообработки; - способы обработки исключительных ситуаций; - терминологию, основные руководящие и регламентирующие документы в области ЭВМ, комплексов и систем; - осуществлять сбор, обработку, анализ и систематизацию научно-технической информации в области ЭВМ и систем с применением современных информационных технологий ; - современные технологии и методы программирования	- формировать требования и разрабатывать внешние спецификации для разрабатываемого программного обеспечения ; - работать с интегрированной средой разработки программного обеспечения; - использовать шаблоны классов и средства макрообработки; - использовать динамически подключаемые библиотеки.	- навыками проектирования программного обеспечения с использованием средств автоматизации; - навыками разработки программной документации
способность понимать значение информации в развитии современного общества, применять достижения современных информационных	- основные понятия информатики; - формы и способы представления данных в персональном компьютере; - состав, назначение функциональных компонентов и программного обеспечения персонального компьютера; - классификацию современных компьютерных систем;	- пользоваться сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети Интернет	-профессиональной терминологией в области информационной безопасности; -навыками разработки, документирования, тестирования и отладки программного обеспечения в соответствии с современными

технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах(ОПК-4)	- типовые структуры и принципы организации компьютерных сетей		технологиями и методами программирования
способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ОПК-5)	– методологии и методы проектирования программного обеспечения; – принципы работы элементов и функциональных узлов электронной аппаратуры; – основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; – архитектуру, принципы функционирования, элементную базу современных компьютеров, вычислительных и телекоммуникационных систем; – принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей;	– анализировать и применять физические явления и эффекты для решения практических задач обеспечения информационной безопасности; – проектировать структуру и архитектуру программного обеспечения с использованием современных методологий и средств автоматизации проектирования программного обеспечения; – классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; – составлять аналитические обзоры по вопросам обеспечения информационной безопасности автоматизированных систем; – разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем; – составлять аналитические обзоры по вопросам обеспечения информа-	– основами построения математических моделей систем передачи информации; – навыками применения математического аппарата для решения прикладных теоретико-информационных задач; – методами теоретического исследования физических явлений и процессов;

		ционной безопасности автоматизированных систем;	
способность применять нормативные правовые акты в профессиональной деятельности (ОПК-6)	- правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны; - правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации; - основные отечественные и зарубежные стандарты в области информационной безопасности - место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России	- применять действующую законодательную базу в области обеспечения информационной безопасности - классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности	- навыками работы с нормативными правовыми актами
способность применять приемы первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций (ОПК-7)	- опасные и вредные факторы системы «человек - среда обитания»; - научные и организационные основы защиты окружающей среды и ликвидации последствий аварий, катастроф, стихийных бедствий	- 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	- навыками безопасного использования технических средств в профессиональной деятельности

способность к освоению новых образцов программных, технических средств и информационных технологий (ОПК-8)	– типовые структуры и принципы организации компьютерных сетей; – общие принципы построения и использования современных языков программирования высокого уровня; – современные технологии и методы программирования; – принципы построения и функционирования, примеры реализаций современных операционных систем; – последовательность и содержание этапов построения компьютерных сетей; – технические характеристики, показатели качества ЭВМ и систем, методы их оценки и пути совершенствования; – состав, назначение функциональных компонентов и программного обеспечения персонального компьютера; – классификацию современных компьютерных систем;	– проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы; – пользоваться сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети Интернет; – работать с интегрированной средой разработки программного обеспечения; – формировать требования и разрабатывать внешние спецификации для разрабатываемого программного обеспечения; – проектировать и администрировать компьютерные сети, реализовывать политику безопасности компьютерной сети; – разрабатывать и администрировать базы данных и интерфейсы прикладных программ к базам данных; – разрабатывать прикладные программы, осуществляющие взаимодействие с базами данных; – применять средства обеспечения безопасности данных;	– методами теоретического исследования физических явлений и процессов; – навыками работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов); – 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; – криптографической терминологией; – навыками использования типовых криптографических алгоритмов; – навыками использования ЭВМ в анализе простейших шифров; – навыками математического моделирования в криптографии; навыками работы с технической документацией на ЭВМ и вычислительные системы;

Профессиональные компетенции (ПК) в научно-исследовательской деятельности			
способность осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке (ПК-1)	- состав, назначение функциональных компонентов и программного обеспечения персонального компьютера; - типовые структуры и принципы организации компьютерных сетей; – терминологию, основные руководящие и регламентирующие документы в области ЭВМ, комплексов и систем; – 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; – лексический и грамматический минимум в объеме, необходимом для работы с текстами профессиональной направленности и осуществления коммуникации на иностранном языке;	– осуществлять сбор, обработку, анализ и систематизацию научно-технической информации в области ЭВМ и систем с применением современных информационных технологий; – составлять аналитические обзоры по вопросам обеспечения информационной безопасности автоматизированных систем; – читать и переводить научно-техническую литературу на иностранном языке по профессиональной тематике, правильно употреблять терминологическую лексику в профессиональной речи; - разрабатывать проекты нормативных материалов, 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 технические задания на создание подсистем информационной безопасности	– навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности; – навыками работы с технической документацией на компоненты автоматизированных систем на русском и иностранном языках; - иностранным языком в объёме, необходимом для получения и изложения информации по профессиональной тематике, навыками общения на иностранном языке; -навыками работы с технической документацией на компоненты автоматизированных систем на русском и иностранном языках

		автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов; - 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	
способность создавать и исследовать модели автоматизированных систем (ПК-2)	– основные информационные технологии, используемые в автоматизированных системах; – методы анализа и синтеза электронных схем; – типовые схемотехнические решения основных узлов и блоков электронной аппаратуры; – эталонную модель взаимодействия открытых систем; – 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 автома-	– разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем; – исследовать эффективность создаваемых средств автоматизации, проводить технико-экономическое обоснование проектных решений;	– навыками анализа основных узлов и устройств современных автоматизированных систем; – методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем; -навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности;

	тизированных систем и подсистем безопасности автоматизированных систем;		
способность проводить анализ защищенности автоматизированных систем (ПК-3)	– средства обеспечения безопасности данных; – основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; – автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности; - методы аттестации уровня защищенности автоматизированных систем	- оценивать эффективность и надежность защиты систембаз данных; – эффективно использовать различные методы и средства защиты информации для компьютерных сетей; – реализовывать политику безопасности баз данных; – применять средства обеспечения безопасности данных; – применять знания о системах электрической связи для решения задач по созданию защищенных телекоммуникационных систем; – определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите;	– 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 анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем; -методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем;
способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы (ПК-4)	- основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в компьютерных сетях; – источники и классификацию угроз информационной безопасности; – основные задачи и понятия криптографии; – требования к шифрам и основные характеристики шифров; – типовые поточные и блочные шифры;	– эффективно использовать различные методы и средства защиты информации для компьютерных сетей; – реализовывать политику безопасности баз данных; – применять средства обеспечения безопасности данных; – анализировать и оценивать угрозы 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; – методами и технологиями мо-

	– 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; – способы кодирования информации; – основные телекоммуникационные протоколы; – основные угрозы безопасности информации и модели нарушителя в автоматизированных системах;	объекта; – разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем;	ниторинга угроз безопасности компьютерных сетей;
способность проводить анализ рисков информационной безопасности автоматизированной системы (ПК-5)	-Сущность и понятие информации, информационной безопасности и характеристику ее составляющих;	– анализировать тенденции развития систем и сетей электросвязи, внедрения новых служб и услуг связи; – выявлять уязвимости информационно-технологических ресурсов автоматизированных систем, проводить мониторинг угроз безопасности автоматизированных систем; – оценивать информационные риски в автоматизированных системах;	- методами оценки информационных рисков;
способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения	– основные информационные технологии, используемые в автоматизированных системах; – принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей; – принципы построения и функционирования, архитектуру, примеры реализаций современных систем управления базами данных;	- реализовывать политику безопасности баз данных; – проводить анализ архитектуры и структуры ЭВМ и систем, оценивать эффективность архитектурно-технических решений, реализованных при построении ЭВМ и систем;	- методами формирования требований по защите информации; - навыками анализа основных узлов и устройств современных автоматизированных систем;

автоматизированных систем в сфере профессиональной деятельности (ПК-6)	– основные задачи и понятия криптографии; – требования к шифрам и основные характеристики шифров; – типовые поточные и блочные шифры; – частотные характеристики открытых текстов и способы их применения к анализу простейших шифров замены и перестановки; – типовые шифры с открытыми ключами; – модели шифров и математические методы их исследования; – технические характеристики, показатели качества ЭВМ и систем, методы их оценки и пути совершенствования; – методы, способы и средства обеспечения отказоустойчивости автоматизированных систем;	– анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем; – анализировать тенденции развития систем и сетей электросвязи, внедрения новых служб и услуг связи; – разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем; - определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; - определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем, составлять аналитические обзоры по вопросам обеспечения	- навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем; - навыками участия в экспертизе состояния защищенности информации на объекте защиты

		информационной безопасности автоматизированных систем	
способность разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ (ПК-7)	– принципы организации документирования разработки, процесса сопровождения программного обеспечения; – последовательность и содержание этапов проектирования баз данных; – последовательность и содержание этапов построения компьютерных сетей; – основные задачи и понятия криптографии; – требования к шифрам и основные характеристики шифров; – типовые поточные и блочные шифры; – частотные характеристики открытых текстов и способы их применения к анализу простейших шифров замены и перестановки; – типовые шифры с открытыми ключами; – модели шифров и математические методы их исследования; – терминологию, основные руководящие и регламентирующие документы в области ЭВМ, комплексов и систем; – основные положения стандартов Единой системы конструкторской документации, Единой системы программной документации;	– осуществлять сбор, обработку, анализ и систематизацию научно-технической информации в области ЭВМ и систем с применением современных информационных технологий; – составлять аналитические обзоры по вопросам обеспечения информационной безопасности автоматизированных систем; – применять требования Единой системы конструкторской документации и Единой системы программной документации при разработке технической документации;	- навыками разработки технической документации в соответствии с требованиями Единой системы конструкторской документации и Единой системы программной документации; – навыками разработки программной документации; – навыками работы с технической документацией на ЭВМ и вычислительные системы; - навыками разработки технической документации в соответствии с требованиями Единой системы конструкторской документации и Единой системы программной документации;
в проектно-конструкторской деятельности:			
способность разрабатывать и анализировать проектные решения по обеспечению	– 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	-оценивать информационные риски в автоматизированных системах; – анализировать и применять физические явления и эффекты для ре-	– основами построения математических моделей систем передачи информации; – навыками применения математического аппарата для решения прикладных теоретико-инфор-

безопасности автоматизированных систем (ПК-8)	источников информации и помехоустойчивого кодирования каналов связи; – основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в компьютерных сетях; – принципы построения и функционирования, архитектуру, примеры реализаций современных систем управления базами данных; – средства обеспечения безопасности данных; – 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; – принципы построения и функционирования систем и сетей передачи информации; – программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, компьютерных сетях; – методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем; – основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения информационной безопасности в автоматизированных и телекоммуникационных системах;	шения практических задач обеспечения информационной безопасности; – применять на практике методы анализа электрических цепей; – 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; – реализовывать политику безопасности баз данных; – применять средства обеспечения безопасности данных; – применять знания о системах электрической связи для решения задач по созданию защищенных телекоммуникационных систем; – разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов;	мационных задач; – навыками обеспечения безопасности информации с помощью типовых программных средств (антивирусов, архиваторов, стандартных сетевых средств обмена информацией); – 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; – 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;
способность участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности (ПК-9)	– 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 программного обеспечения персонального компьютера; – язык программирования высокого уровня (объектно-ориентированное программирование); – основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты 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; – автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности; – методы, способы, средства, последовательность и содержание этапов разработки автома-	– анализировать и применять физические явления и эффекты для решения практических задач обеспечения информационной безопасности; – 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; – эффективно использовать различные методы и средства защиты информации для компьютерных сетей; – реализовывать политику безопасности баз данных; – эффективно использовать криптографические методы и средства защиты информации в автоматизи-	– навыками применения математического аппарата для решения прикладных теоретико-информационных задач; – методами и средствами технической защиты информации; – навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем; - методами теоретического исследования физических явлений и процессов;

	тизированных систем и подсистем безопасности автоматизированных систем; – основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические);	рованных системах; – проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы;	
способность применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности (ПК-10)	- принципы работы элементов современной радиоэлектронной аппаратуры и физические процессы, протекающие в них; - основы схемотехники современной радиоэлектронной аппаратуры; - методы анализа и синтеза электронных схем; - основы теории электрических цепей; - принципы работы элементов и функциональных узлов электронной аппаратуры; типовые схемотехнические решения основных узлов и блоков электронной аппаратуры; - методы анализа и синтеза электронных схем; - основы теории электрических цепей; - принципы работы элементов и функциональных узлов электронной аппаратуры; типовые схемотехнические решения основных узлов и блоков электронной аппаратуры	- применять на практике методы анализа электрических цепей; - использовать стандартные методы и средства проектирования цифровых узлов и устройств, в том числе для средств защиты информации; - проектировать структуру и архитектуру программного обеспечения с использованием современных методологий и средств автоматизации проектирования программного обеспечения проводить выбор эффективных способов реализации структур данных и конкретных алгоритмов при решении профессиональных задач; - применять знания о	- навыками работы с программными средствами схемотехнического моделирования; - навыками разработки, документирования, тестирования и отладки программного обеспечения в соответствии с современными технологиями и методами программирования; - навыками проектирования программного обеспечения с использованием средств автоматизации; - навыками разработки программной документации; - навыками программирования с использованием эффективных реализаций структур данных и

		системах электрической связи для решения задач по созданию защищенных телекоммуникационных систем	алгоритмов
способность разрабатывать политику информационной безопасности автоматизированной системы (ПК-11)	- основные угрозы безопасности информации и модели нарушителя в автоматизированных системах - принципы формирования политики информационной безопасности в автоматизированных системах; – 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; – 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 предпри-	- определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; - разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем разрабатывать частные политики информационной безопасности информационной безопасности автоматизированных систем; – планировать политику безопасности операционных систем; – проектировать и администрировать компьютерные сети, реализовывать политику безопасности компьютерной сети; – эффективно использовать различные методы и средства защиты информации для компьютерных сетей; – реализовывать политику безопасности баз данных; – применять средства обеспечения	- навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности; – навыками разработки, документирования компьютерных сетей с учетом требований по обеспечению безопасности; – 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;

	ятиях; – 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; – принципы формирования политики информационной безопасности в автоматизированных системах;	безопасности данных; – классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; – классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; – разрабатывать частные политики информационной безопасности автоматизированных систем; – контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем;	
способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы (ПК-12)	– методологии и методы проектирования программного обеспечения; – методы тестирования и отладки программного обеспечения; – 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; – функции операционных систем, основные концепции управления процессорами, памятью, вспомогательной памятью, устройствами; – основные методы управления информационной безопасностью;	- оценивать информационные риски в автоматизированных системах; – вычислять теоретико-информационные характеристики источников сообщений и каналов связи; - разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем	– основами построения математических моделей систем передачи информации; – навыками обеспечения безопасности информации с помощью типовых программных средств (антивирусов, архиваторов, стандартных сетевых средств обмена информацией); – навыками анализа основных характеристик и возможностей телекоммуникационных систем по передаче информации; - методами управления информационной безопасностью автоматизированных систем;

способность участвовать в проектировании средств защиты информации автоматизированной системы (ПК-13)	- требования к шифрам и основные характеристики шифров; типовые поточные и блочные шифры; - 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; - 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; -физические явления и эффекты, используемые при обеспечении информационной безопасности автоматизированных систем; – основные протоколы компьютерных сетей; – эталонную модель взаимодействия открытых систем; – основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; – автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее ин-	- эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах; - исследовать эффективность создаваемых средств автоматизации, проводить техникоэкономическое обоснование проектных решений; - разрабатывать частные политики информационной безопасности автоматизированных систем – анализировать и применять физические явления и эффекты для решения практических задач обеспечения информационной безопасности; – использовать стандартные методы и средства проектирования цифровых узлов и устройств, в том числе для средств защиты информации; – реализовывать политику безопасности баз данных; – эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах; – применять знания о системах электрической связи для решения задач по созданию защищенных те-	- криптографической терминологией; - методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем; -методами и средствами технической защиты информации; -методами теоретического исследования физических явлений и процессов; – навыками разработки, документирования компьютерных сетей с учетом требований по обеспечению безопасности; – навыками использования программно-аппаратных средств обеспечения безопасности компьютерных сетей; – методами расчета и инструментального контроля показателей технической защиты информации; - навыками анализа основных характеристик и возможностей телекоммуникационных систем по передаче информации

	формационной безопасности; – методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем; – основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические);	лекоммуникационных систем; – проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы; – разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов;	
в контрольно-аналитической деятельности			
способность проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-14)	-требования к шифрам и основные характеристики шифров; - основные информационныетехнологии, используемые в автоматизированных системах; – критерии оценки эффективности и надежности средств защиты операционных систем; – основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в компьютерных сетях; – 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 информа-	-контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем; – эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах; – применять математические методы исследования моделей шифров; – администрировать подсистемы информационной безопасности автоматизированных систем;	- навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем; - методами расчета и инструментального контроля показателей технической защиты информации; - навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности;

	тизации; – 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;		- методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем; методами оценки информационных рисков; – навыками использования измерительного оборудования при экспериментальном исследовании электронной аппаратуры; – навыками работы с программными средствами схемотехнического моделирования; – методами и средствами технической защиты информации; – методами расчета и инструментального контроля показателей технической защиты информации; – навыками поддержания работоспособности, обнаружения и устранения неисправностей в работе электронных аппаратных средств автоматизированных систем; - навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем;
способность участвовать в	– основы теории электрических цепей; – принципы работы элементов и функциональ-	– применять на практике методы анализа электрических цепей;	- методами расчета и инструментального контроля пока-

проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем (ПК15)	ных узлов электронной аппаратуры; – методы анализа и синтеза электронных схем; – типовые схемотехнические решения основных узлов и блоков электронной аппаратуры; – 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; – методы аттестации уровня защищенности автоматизированных систем; - способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; - возможности технических средств перехвата информации	– работать с современной элементной базой электронной аппаратуры; использовать стандартные методы и средства проектирования цифровых узлов и устройств, в том числе для средств защиты информации; – эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах; – составлять аналитические обзоры по вопросам обеспечения информационной безопасности автоматизированных систем;	зателей технической защиты информации;
способность участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных требований по защите информации (ПК-16)	– 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; – способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; – основные характеристики сигналов электросвязи, спектры и виды модуляции; – основы организационного и правового обеспечения информационной безопасности, основные	- работать с современной элементной базой электронной аппаратуры; – разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем; – выявлять уязвимости информационно-технологических ресурсов автоматизированных систем, проводить мониторинг угроз безопасности автоматизированных систем; – эффективно использовать различные методы и средства защиты ин-	– методами формирования требований по защите информации; – методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем; – навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности; – методами мониторинга и аудита, выявления угроз информационной безопасности автоматизи-

	нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации; – 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;	формации для компьютерных сетей;	рованных систем; - навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем;
способность проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации (ПК-17)	- технические каналы утечки информации; – физические явления и эффекты, используемые при обеспечении информационной безопасности автоматизированных систем; – 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 аттестации уровня защищенности автоматизированных систем;	– анализировать и применять физические явления и эффекты для решения практических задач обеспечения информационной безопасности; – анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем; – разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации; – проводить мониторинг угроз безопасности компьютерных сетей;	- методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем; – навыками проведения физического эксперимента и обработки его результатов; – профессиональной терминологией в области информационной безопасности; – методами расчета и инструментального контроля показателей технической защиты информации; – навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем; - методами мониторинга и аудита, выявления угроз ин-

			формационной безопасности автоматизированных систем;
в организационно-управленческой деятельности			
способность организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности (ПК-18)	- основные понятия и методы в области управленческой деятельности; порядок выработки и реализации управленческих решений; - содержание управленческой работы руководителя подразделения; - содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем; - научные основы, цели, принципы, методы и технологии управленческой деятельности; - принципы организации документирования разработки, процесса сопровождения программного обеспечения; - терминологию, основные руководящие и регламентирующие документы в области ЭВМ, комплексов и систем; - методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем; - основные положения стандартов Единой системы конструкторской документации, Единой системы программной документации;	- оценивать эффективность управленческих решений и анализировать экономические показатели деятельности подразделения; - осуществлять планирование и организацию работы рабочего коллектива при выполнении поставленных задач; - контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем; - администрировать подсистемы информационной безопасности автоматизированных систем; - работать в коллективе, принимать управленческие решения и оценивать их эффективность; - разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов;	- навыками обоснования, выбора, реализации и контроля результатов управленческого решения; - навыками организации и обеспечения режима секретности; - навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности; - навыками выбора, обоснования, реализации и контроля результатов управленческого решения; – навыками работы с нормативными правовыми актами; – навыками организации и обеспечения режима секретности; – методами организации и управления деятельностью служб защиты информации на предприятии; - навыками разработки технической документации в соответствии с требованиями Единой системы конструкторской документации и Единой системы программной доку-

		- определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; - определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем; - применять требования Единой системы конструкторской документации и Единой системы программной документации при разработке технической документации; -	ментации;
способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы (ПК-19)	- состав системы управления и требования к ее элементам; – основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; – основные методы управления информационной безопасностью;	– эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах; – применять математические методы исследования моделей шифров; – применять знания о системах электрической связи для решения задач по созданию защищенных телекоммуникационных систем; - разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем;	- методами управления информационной безопасностью автоматизированных систем;

способность организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности (ПК-20)	- программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, компьютерных сетях; - содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем; -	– проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы; – применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; – администрировать подсистемы информационной безопасности автоматизированных систем; – выявлять уязвимости информационно-технологических ресурсов автоматизированных систем, проводить мониторинг угроз безопасности автоматизированных систем;	- навыками обоснования, выбора, реализации и контроля результатов управленческого решения; - навыками работы с нормативными правовыми актами; - навыками эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечениюинформационной безопасности; - навыками использования программно-аппаратных средств обеспечения безопасности сетей ЭВМ; - 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 использования программно-аппаратных средств обеспечения безопасности компьютерных сетей; - навыками поддержания работоспособности, обнаружения и устранения неисправностей в работе электронных аппаратных средств автоматизированных систем; - методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем;
способность разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем (ПК-21)	- 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; – основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и норма-	- разрабатывать, реализовывать, оценивать и корректировать процессы менеджмента информационной безопасности; - разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем; - использовать в практической деятельности правовые знания, анализировать основные правовые акты, давать правовую оценку ин-	- навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности; – навыками разработки, документирования компьютерных сетей с учетом требований по обеспечению безопасности; – навыками разработки, документирования баз данных с учетом требований по обеспечению информационной безопасности; – навыками работы с нормативными правовыми актами; – навыками организации и обес-

	тивные 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;	формации, используемой в профессиональной деятельности; – разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации;	печения режима секретности; – методами организации и управления деятельностью служб защиты информации на предприятии; - методами формирования требований по защите информации;
способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации (ПК22)	- основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; - принципы формирования политики информационной безопасности в автоматизированных системах; - научные основы, цели, принципы, методы и технологии управленческой деятельности; -сущность и понятие информации, информационной безопасности и характеристику ее составляющих; - 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;	- контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем; - разрабатывать частные политики информационной безопасности автоматизированных систем; - планировать политику безопасности операционных систем; - проектировать и администрировать компьютерные сети, реализовывать политику безопасности компьютерной сети; - разрабатывать частные политики информационной безопасности автоматизированных систем; - контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем;	- навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности; - навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем; - навыками выбора, обоснования, реализации и контроля результатов управленческого решения; - навыками разработки, документирования компьютерных сетей с учетом требований по обеспечению безопасности; - методами формирования требований по защите информации; - методами управления ин-

	- принципы формирования политики информационной безопасности в автоматизированных системах; -	-	формационной безопасностью автоматизированных систем;
способность формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа (ПК23)	– основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; – 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;	- 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; - реализовывать политику безопасности баз данных;	– навыками разработки, документирования компьютерных сетей с учетом требований по обеспечению безопасности; – навыками разработки, документирования баз данных с учетом требований по обеспечению информационной безопасности; – 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 использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем; – методами мониторинга и аудита, выявления угроз информаци-

			онной безопасности автоматизированных систем; – методами управления информационной безопасностью автоматизированных систем; – методами оценки информационных рисков; - навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем;
в эксплуатационной деятельности			
способность обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности (ПК-24)	- основы организационного и правового обеспечения информационной безопасности, основные положения законодательства Российской Федерации в области защиты информации; - основные методы управления информационной безопасностью; – 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;	- восстанавливать работоспособность подсистемы информационной безопасности автоматизированных систем в нештатных ситуациях; - разрабатывать частные политики информационной безопасности автоматизированных систем; – проводить мониторинг угроз безопасности компьютерных сетей;	- навыками организации и обеспечения режима секретности навыками работы с технической документацией на компоненты автоматизированных систем на русском и иностранном языках; - навыками поддержания работоспособности, обнаружения и устранения неисправностей в работе электронных аппаратных средств автоматизированных систем; - навыками использования программно-аппаратных средств обеспечения информационной безопасности

			автоматизированных систем; – навыками анализа основных характеристик и возможностей телекоммуникационных систем по передаче информации; – навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем; – навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности; - навыками анализа основных узлов и устройств современных автоматизированных систем;
способность обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении	- основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в сетях ЭВМ; – средства обеспечения безопасности данных; – основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; – критерии оценки эффективности и надежности средств защиты операционных систем; – программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, компьютерных сетях;	- использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем; - оценивать эффективность и надежность защиты операционных систем; - планировать политику безопасности операционных систем; - эффективно использовать различные методы и средства	- 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;

нештатных ситуаций (ПК25)		защиты информации для компьютерных сетей; - применять средства обеспечения безопасности данных; - проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы; - применять средства обеспечения безопасности данных;	-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;
способность администрировать подсистему информационной безопасности автоматизированной системы (ПК-26)	- 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; содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем; - основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические,	- планировать политику безопасности операционных систем; - применять средства обеспечения безопасности данных; -администрировать подсистемы информационной безопасности автоматизированных систем - реализовывать политику безопасности баз данных;	- 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; - навыками, эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и

	технические); – основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения информационной безопасности в автоматизированных и телекоммуникационных системах; – автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности; – методы, способы и средства обеспечения отказоустойчивости автоматизированных систем; – основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические);		аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности; - навыками использования программно-аппаратных средств обеспечения безопасности сетей ЭВМ; - 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
способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности	– 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 деятель-	- реализовывать политику безопасности баз данных; – проектировать и администрировать компьютерные сети, реализовывать политику безопасности компьютерной сети; – проводить мониторинг угроз безопасности компьютерных сетей; – реализовывать политику безопасности баз данных;	- навыками разработки, документирования баз данных с учетом требований по обеспечению информационной безопасности;

автоматизированной системы (ПК-27)	ности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации; – методы аттестации уровня защищенности автоматизированных систем; – принципы формирования политики информационной безопасности в автоматизированных системах; – основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические);		
способность управлять информационной безопасностью автоматизированной системы (ПК-28)	-основные методы управления информационной безопасностью; – источники и классификацию угроз информационной безопасности; – основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; – 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	-разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем; – выявлять уязвимости информационно-технологических ресурсов автоматизированных систем, проводить мониторинг угроз безопасности автоматизированных систем; – оценивать информационные риски в автоматизированных системах; – составлять аналитические обзоры по вопросам обеспечения информационной безопасности автоматизированных систем;	-методами управления информационной безопасностью автоматизированных 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 систем; – методами управления инфор-

		– разрабатывать частные политики информационной безопасности автоматизированных систем; – контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем; – разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем;	мационной безопасностью автоматизированных систем; - методами оценки информационных рисков;
Профессионально-специализированные компетенции (ПСК)			
способность разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах (ПСК-7.1)	– общую постановку задач математического программирования, динамического программирования, сетевого планирования, теории; игр; - универсальные приемы исследования оптимизационных проблем при различной степени неопределенности условий; – основные информационные технологии, используемые в автоматизированных системах; – способы обеспечения информационной безопасности систем организационного управления; – специфику математического моделирования организационных задач в автоматизированных системах;	– 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; – определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; – выявлять уязвимости информационно-технологических ресурсов автоматизированных систем, прово-	– 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 семантического моделирования данных, навыками проектирования информационных систем на базе корпоративных систем управления базами данных, метода-

		дить мониторинг угроз безопасности автоматизированных систем; – разрабатывать модели систем организационного управления; – 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 и оценивать угрозы информационной безопасности объекта; – разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем; – выявлять уязвимости информационно-технологических ресурсов автоматизированных систем, проводить мониторинг угроз безопасности автоматизированных систем; – разрабатывать модели систем организационного управления;	ми снижения угроз безопасности информационных систем, вызванных ошибками на этапе проектирования, разработки и внедрения;
способностьпроводить анализ рисков информационной безопасности и	– специфику математического моделирования организационных задач в автоматизированных системах; – способы обеспечения информационной безопас-	– анализировать и оценивать угрозы информационной безопасности объекта; – оценивать информационные рис-	- методами оценки информационных рисков; - навыками семантического моделирования данных, на-

разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах (ПСК-7.2)	ности систем организационного управления;	ки в автоматизированных системах; – разрабатывать модели систем организационного управления; – определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем; – разрабатывать частные политики информационной безопасностиавтоматизированных систем; – использовать технологии автоматизированного проектирования и структурный подход при проектировании информационных систем, определять ресурсы, необходимые для обеспечения безопасности информационной системы, использовать методы и средства определения технологической безопасности функционирования распределенной информационной системы;	выками 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 политики безопасности систем организационного управления;
способность проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем (ПСК-7.3)	– методы аттестации уровня защищенности автоматизированных систем; – нормативные документы по метрологии, стандартизации и сертификации программных и аппаратных средств защиты;	– применять нормативные документы по метрологии, стандартизации и сертификации на практике; – использовать технологии автоматизированного проектирования и структурный подход при проектировании информационных систем, определять ресурсы, необходимые для обеспечения безопасности информа-	– методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем; – навыками разработки документации по метрологии, стандартизации и сертификации программных и аппаратных средств защиты;

		ционной системы, использовать методы и средства определения технологической безопасности функционирования распределенной информационной системы;	
способность проводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах (ПСК-7.4)	– 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; – 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; –	– оценивать эффективность и надежность защиты операционных систем; – планировать политику безопасности операционных систем; – использовать технологии автоматизированного проектирования и структурный подход при проектировании информационных систем, определять ресурсы, необходимые для обеспечения безопасности информационной системы, использовать методы и средства определения технологической безопасности функционирования распределенной информационной системы; – разрабатывать и администрировать базы данных и интерфейсы прикладных программ к базам данных; – использовать технологии автоматизированного проектирования и структурный подход при проектировании информационных систем, определять ресурсы, необходимые для обеспечения безопасности информационной системы, использовать методы и средства определения техно-	- 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; –

		логической безопасности функционирования распределенной информационной системы;	
способность координировать деятельность подразделений и специалистов по защите информации на предприятии, в учреждении, организации (ПСК-7.5)	– содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем; – основные положения теории управления;	работать в коллективе, принимать управленческие решения и оценивать их эффективность;	– навыками разработки политики безопасности систем организационного управления;

4. ДОКУМЕНТЫ, РЕГЛАМЕНТИРУЮЩИЕ СОДЕРЖАНИЕ И ОРГАНИЗАЦИЮ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПРИ РЕАЛИЗАЦИИ ДАННОЙ ООП ВО

4.1. Программные документы интегрирующего, междисциплинарного и сквозного характера, обеспечивающие целостность компетентностно - ориентированной ООП ВО

4.1.1. Календарный учебный график и учебный план подготовки специалиста
(Приложение 1)
4.1.2. Компетентностно - ориентированный учебный план
(Приложение 2)
4.2. Дисциплинарно - модульные программные документы компетентностно - ориентированной ОП ВО
4.2.1. Аннотации и рабочие программы учебных курсов, предметов, дисциплин (модулей)
(Приложение 3)

5. РЕСУРСНОЕ ОБЕСПЕЧЕНИЕ ООП ВО СПЕЦИАЛИТЕТА ПО НАПРАВЛЕНИЮ

5.1. Учебно-методическое и информационное обеспечение образовательного процесса при реализации ОП

Основная образовательная программа специалитета обеспечена учебно - методической документацией и материалами по всем учебным курсам, дисциплинам (модулям) основной образовательной программы. Аннотации всех учебных дисциплин (курсов, модулей) представлено в сети Интернет.

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 расчета не менее 25 экземпляров таких изданий на каждые 100 обучающихся.

Фонд дополнительной литературы, помимо учебной, включает официальные, справочно – библиографические и специализированные периодические издания.

Фонд научной литературы представлен монографиями, периодическими научными изданиями по профилю образовательной

программы.

По данной основной образовательной программе имеются изданные в БГТУ им. В.Г. Шухова учебные пособия по дисциплинам учебного плана, в том числе издания с грифом УМО. Учебный процесс обеспечен методическими разработками по выполнению лабораторных работ, курсовых работ, для обеспечения самостоятельной работы студентов, итоговой аттестации выпускников. По ряду дисциплин учебного плана методические разработки представлены в виде электронного ресурса, входящего в состав учебно-методических комплексов дисциплин и размещены на информационном сайте выпускающей кафедры «Программное обеспечение вычислительной техники и автоматизированных систем».

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

Каждый обучающийся обеспечен доступом к электронно – библиотечной системе, содержащей полные тексты учебников и учебных пособий, изданных авторами БГТУ им. В.Г. Шухова; к электронным базам ведущих информационных центров: «Кодекс», «Консультант Плюс», «НормаCS». Организована работа виртуального читального зала диссертаций, хранящихся в Российской государственной библиотеке; также предоставлен доступ к полным текстам иностранных журналов РФФИ, базе данных экономики и права «Polpred», электронной библиотеке НИТУ МИСиС, Электронно-библиотечной системе «КнигаФонд».

Библиотека имеет собственный web-сайт (http://ntb.bstu.ru/), информирующий о ресурсах и услугах библиотеки.

Оперативный обмен информацией с отечественными и зарубежными вузами и организациями осуществляется с соблюдением требований законодательства Российской Федерации об интеллектуальной собственности и международных договоров Российской Федерации в области интеллектуальной собственности.

5.2. Кадровое обеспечение реализации ОП

Реализация основной образовательной программы специалитета обеспечивается научно – педагогическими кадрами, имеющими базовое образование, соответствующее профилю преподаваемой дисциплины, и систематически занимающимися научной и научно - методической деятельностью.

Доля штатных научно-педагогических работников составляет 86%.

Доля преподавателей, имеющих ученую степень и ученое звание, составляет 71 %. Доля преподавателей, имеющих образование или ученую степень, соответствующие профилю преподаваемой дисциплины, составляет 87 % .

К образовательному процессу привлечены преподаватели из числа действующих руководителей и работников профильных организаций. Доля

преподавателей из числа руководителей и работников организаций, деятельность которых связана со специализацией реализуемой программы специалитета, составляет 5,9 %.

Кадровый состав, реализующий ОП, представлен в Приложении 4.

5.3. Основные материально - технические условия для реализации образовательного процесса в вузе в соответствии с ОП ВО

Материально-техническая база университета обеспечивает условия для проведения всех видов дисциплинарной и междисциплинарной подготовки, лабораторной, практической и научно-исследовательской работы обучающихся, предусмотренных учебным планом и соответствующими действующими санитарными и противопожарными правилами и нормами.

Перечень материально-технического обеспечения включает в себя специально оборудованные кабинеты, учебные лаборатории и классы, оснащенные современными компьютерами, объединенными в локальные вычислительные сети с выходом в Интернет. В учебном процессе используются лаборатории:

- лаборатория сетей и систем передачи информации ;
- лаборатория безопасности сетей ЭВМ;
- лаборатория технической защиты информации;
- лаборатория программно-аппаратных средств обеспечения информационной безопасности;
- лаборатория технологий и методов программирования;
- лаборатория электротехники и электроники;
- лаборатории в области физики:
  - лаборатория механики;
  - лаборатория электричества и магнетизма;
  - лаборатория оптики;
  - лаборатория физики твердого тела;
  - лаборатория молекулярной физики;
- компьютерные залы.

Перечень оборудования лабораторий представлен в Приложении 5.

Компьютерные классы оснащены периферийным, проекционным оборудованием, интерактивными досками и предоставляют дистанционный доступ к учебной и научной информации. Практические занятия проводятся с применением современных программно -методических комплексов для получения знаний и приобретения навыков решения задач по всем видам профессиональной и естественнонаучной подготовки. Студенту предоставлена возможность практической работы на ЭВМ различной архитектуры в среде различных операционных систем и средств разработки программных и информационных систем.

При использовании электронных изданий, во время самостоятельной подготовки, обучающиеся обеспечены рабочими местами в компьютерном классе с выходом в Интернет в соответствии с объемом изучаемых дисциплин.

Учебный процесс обеспечен лицензионным и свободно распространяемым программным обеспечением.

Лабораторные и практические занятия по дисциплинам профессионального цикла проводятся в учебных лабораториях программно - аппаратных средств обеспечения информационной безопасности, технологии и методов программирования, сетей и систем передачи информации, безопасности сетей ЭВМ, технической защиты информации.

Учебная практика проводится в лабораториях и классах вуза, производственная практика организуется на базе промышленных предприятий, проектных, государственных, муниципальных, общественных и других организаций Белгорода, Белгородской области и других регионов.

6. ХАРАКТЕРИСТИКИ СОЦИАЛЬНО - КУЛЬТУРНОЙ СРЕДЫ ВУЗА, ОБЕСПЕЧИВАЮЩИЕ РАЗВИТИЕ ОБЩЕКУЛЬТУРНЫХ (СОЦИАЛЬНО - ЛИЧНОСТНЫХ) КОМПЕТЕНЦИЙ ВЫПУСКНИКОВ

Для всестороннего развития личности и регулирования социально-культурных процессов, способствующих укреплению нравственных, гражданственных, общекультурных качеств студентов в ФГОУ ВО «БГТУ им. В.Г. Шухова» сформирована соответствующая социально - культурная среда. В соответствии с планами культурно - воспитательной работы, реализуемыми университетом, институтами и кафедрами, предусмотрены индивидуальная воспитательная работа, кураторская работа в группах, студенческое самоуправление, организуются научно - практические, воспитательные, развлекательные и спортивные мероприятия. Для формирования общекультурных компетенций (компетенций социального взаимодействия, самоорганизации и самоуправления, компетенций системно - деятельностного характера) сформированы условия, стимулирующие студентов к участию в органах самоуправления, работе студенческих строительных отрядах, благотворительных акциях, творческих клубах, студенческих научных обществах и т.д.

Особое внимание уделяется студенческому самоуправлению, что дает широкие возможности для реализации личностного потенциала студентов. В ФГОУ ВО «БГТУ им. В.Г. Шухова» функционируют студенческие советы университета, институтов и общежития. Руководящим органом системы студенческого самоуправления является Студенческий совет, предоставляющий обучающемуся возможность развивать лидерские качества

будущего управленца, принимать обоснованные решения и нести ответственность за их реализацию.

Студенческой профсоюзной организацией решаются социальные вопросы студентов, осуществляется социальная защита на основе устава профсоюзной организации.

Спортивно - массовая работа со студентами проводится с целью сохранения и приумножения спортивных достижений ФГОУ ВО «БГТУ им. В.Г. Шухова», региона и страны; популяризации различных видов спорта; формирования у студентов культуры здорового образа жизни. Физическая культура и спорт рассматриваются как важная составляющая подготовки квалифицированного бакалавра, востребованного на рынке труда.

Сформированная социально - культурная среда позволяет решать широкий спектр задач, направленных гражданско-патриотическое, духовно-нравственное и эстетическое воспитание студенческой молодежи.

7. НОРМАТИВНО - МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ СИСТЕМЫ ОЦЕНКИ КАЧЕСТВА ОСВОЕНИЯ ОБУЧАЮЩИМИСЯ ООП ВО

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

Текущий контроль успеваемости обеспечивает оценивание хода освоения дисциплин (модулей) и прохождения практик.

Для осуществления текущего контроля, в рамках рабочих программ дисциплин созданы фонды оценочных средств успеваемости, которые включают тесты, контрольные вопросы и типовые задания для практических занятий, лабораторных и контрольных работ, коллоквиумов, зачетов и экзаменов, примерную тематику рефератов и т.п., а также иные формы контроля, позволяющие оценить степень сформированности компетенций обучающихся.

Промежуточная аттестация обучающихся – оценивание промежуточных и окончательных результатов обучения по дисциплинам (модулям), прохождения практик, выполнения научных исследований.

Порядок проведения промежуточной аттестации обучающихся, включая порядок установления сроков прохождения, а также периодичность проведения промежуточной аттестации осуществляется согласно «Положения о промежуточной аттестации БГТУ им. В.Г. Шухова».

7.2. Итоговая государственная аттестация выпускников ООП ВО.

Итоговая аттестация выпускника является обязательной и осуществляется после освоения образовательной программы в полном объеме в соответствии с Положением об итоговой государственной аттестации выпускников университета БГТУ им. В.Г. Шухова.

Итоговая государственная аттестация включает:

- защиту выпускной квалификационной работы.

Образовательная программа обсуждена на заседании выпускающей кафедры ПОВТиАС

«16» 01 2017 г., протокол № 6

Заведующий кафедрой: к.т.н., доцент_____(Поляков В.М.)

Основная образовательная программа согласована:

Первый проректор	Н.А. Шаповалов
Проректор по учебной работе	В.М. Поляков
Начальник учебно-методического управления	Т.А. Дуюн
Начальник управления качества	Е.А. Дороганов

Утверждение изменений в образовательной программе для реализации в 2019/20 учебном году

ООП рассмотрена, обсуждена и одобрена для реализации в 2019/2020 учебном году на заседании Ученого совета университета «25» июня 2019 г. протокол № 13

Председатель Ученого совета: _______________ (Евтушенко Е.И.)
(инициалы, фамилия)

Заведующий кафедрой: _______________ (В.М. Поляков)

Утверждение изменений в образовательной программе для реализации в 20___/___ учебном году

ООП рассмотрена, обсуждена и одобрена для реализации в 20___/20___ учебном году на заседании Ученого совета университета «____» _________ 20____г. протокол №___

Председатель Ученого совета: _______________ (_______________)
(инициалы, фамилия)

Заведующий кафедрой: _______________ (В.М. Поляков)

Утверждение изменений в образовательной программе для реализации в 20___/___ учебном году

ООП рассмотрена, обсуждена и одобрена для реализации в 20___/20___ учебном году на заседании Ученого совета университета «____» _________ 20____г. протокол №___

Председатель Ученого совета: _______________ (_______________)
(инициалы, фамилия)

Заведующий кафедрой: _______________ (В.М. Поляков)

Утверждение изменений в образовательной программе для реализации в 20___/___ учебном году

ООП рассмотрена, обсуждена и одобрена для реализации в 20___/20___ учебном году на заседании Ученого совета университета «____» _________ 20____г. протокол №___

Председатель Ученого совета: _______________ (_______________)
(инициалы, фамилия)

Заведующий кафедрой: _______________ (В.М. Поляков)