Результаты освоения образовательной программы высшего образования, соответствующие ФГОС ВО, и учитывающие требования профессионального стандарта (стандартов)

Планируемые результаты освоения образовательной программы	**Элементы образовательной программы, формирующие результаты освоения**	**Профессиональный стандарт «Специалист по защите информации в автоматизированных системах» (утвержден Приказом Минтруда от 15.09.2016 № 522н)**
ОПК-1 «способностью анализировать физические явления и процессы для решения профессиональных задач»		
Знать: - особенности физических эффектов и явлений, используемых для информационного обеспечения функционирования систем автоматизированной обработки информации и управления; - структурные схемы, назначение и принцип работы электронных устройств, имеющих в своем составе электронные приборы; - принцип действия и применения основных типов аналоговых и цифровых измерительных приборов; Уметь: - производить оценку физических эффектов и явлений, проявляющихся в информационных системах; - решать типовые задачи по определению основных характеристик электротехнических устройств; - использовать основные способы измерений характеристик сигналов, применяемых в информационных системах Владеть:	Физика Аппаратные средства вычислительной техники Электротехника Электроника и схемотехника Метрология и электрорадиоизмерения Концепция современного естествознания Основы радиотехники	Профессиональный стандарт «Специалист по защите информации в автоматизированных системах» (утвержден Приказом Минтруда от 15.09.2016 № 522н) **3.2.1. ТФ:** Диагностика систем защиты информации автоматизированных систем **3.2.3. ТФ:** Управление защитой информации в автоматизированных системах

- методами применения основных законы физики при решении практических задач; - методами проведения физических измерений		
ОПК-2 «способностью применять соответствующий математический аппарат для решения профессиональных задач»		
Знать: - понятие алгоритма и его свойства, виды алгоритмических процессов; - основные алгебраические методы, применяемые в криптологии; - алгебраические модели систем шифрования; - методы и принципы теорий, связанных с решением оптимизационных задач математического программирования; Уметь: − применять различные подходы к алгоритмизации процессов обработки информации; - применять в научно-исследовательской и прикладной деятельности методы математического программирования; − представлять формализованное описание задач оптимизации для построения математических моделей автоматизированных систем и процессов; Владеть: - применением методов полиномиальной алгебры к задачам построения шифрующих программ; - навыками использования прикладных программ общего назначения в целях	Математика Алгебра и геометрия Математический анализ Дискретная математика Математическая логика и теория алгоритмов Математические основы криптологии Вычислительная математика Прикладное программирование Методы оптимизации Методы вычислений Среда моделирования Компьютерная графика	Профессиональный стандарт «Специалист по защите информации в автоматизированных системах» (утвержден Приказом Минтруда от 15.09.2016 № 522н) **3.2.5. ТФ:** Мониторинг защищенности информации в автоматизированных системах **3.2.6. ТФ:** Аудит защищенности информации в автоматизированных системах

решения практических задач оптимизации управленческих процессов		
ОПК-3 «способностью применять положения электротехники, электроники и схемотехники для решения профессиональных задач»		
Знать: - основные понятия метрологии и техники измерений; - классификацию методов измерений, погрешности измерений и технических средств, классы точности приборов и применение их при эксплуатации устройств и средств защиты информации и автоматизации производства; Уметь: − применять математические методы при расчете цепей постоянного и переменного тока; - осуществлять поиск нормативных документов по вопросам технического регулирования защиты информации и автоматизации производства; - подбирать средства измерений удовлетворяющие конкретным требованиям при измерениях; Владеть: - методами проведения физических измерений; - профессиональной терминологией в области техники измерений и технического регулирования; – основными методами измерения и применения электрорадиоизмерительных приборов.	Теория вероятностей и математическая статистика Физика Информатика Теория информации Аппаратные средства вычислительной техники Языки программирования Электротехника Электроника и схемотехника Метрология и электрорадиоизмерения Основы радиотехники Технические средства охраны Технические средства безопасности Учебная практика	Профессиональный стандарт «Специалист по защите информации в автоматизированных системах» (утвержден Приказом Минтруда от 15.09.2016 № 522н) **3.1.1. ТФ:** Проведение регламентных работ по эксплуатации систем защиты информации автоматизированных систем **3.1.2. ТФ:** Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем

ОПК-4 «способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации»		
Знать: - теоретические основы информатики; - современные виды информационного взаимодействия и обслуживания; - основные типы архитектур современных вычислительных систем (ВС) и сетей ЭВМ (вычислительных сетей), принципы их организации и функционирования; Уметь: − развертывать, конфигурировать и настраивать вычислительные сети; - проводить качественное и количественное сравнение систем различных типов при анализе их производительности или эффективности применения для решения задач различных классов - оценивать целесообразность решения прикладных задач в вычислительных сетях Владеть: - навыками использования стандартных информационных технологий для решения профессиональных задач; - информацией об основных направлениях развития исследований в области архитектуры ВС и наиболее значительных перспективных проектах ВС, об основных методах распределенной обработки данных в сетях ЭВМ, о задачах и методах управления, протоколах взаимодействия в вычислительных сетях	Информатика Документоведение Информационные технологии Вычислительная математика Общая теория систем Сети и телекоммуникации Методы оптимизации Методы вычислений Государственная итоговая аттестация	Профессиональный стандарт «Специалист по защите информации в автоматизированных системах» (утвержден Приказом Минтруда от 15.09.2016 № 522н) **3.1.3. ТФ:** Обеспечение защиты информации при выводе из эксплуатации автоматизированных систем **3.3.1. ТФ:** Установка и настройка средств защиты информации в автоматизированных системах

ОПК-5 «способностью использовать нормативные правовые акты в профессиональной деятельности»		
Знать: - основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации; - правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны и служб защиты информации на предприятиях; - цели, задачи, принципы и основные направления обеспечения информационной безопасности государства; Уметь: -применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; - разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации; Владеть: - навыками работы с нормативными правовыми актами; - навыками организации и обеспечения режима конфиденциальности;	Основы информационной безопасности Организационное и правовое обеспечение информационной безопасности Документоведение Учебная практика Государственная итоговая аттестация	Профессиональный стандарт «Специалист по защите информации в автоматизированных системах» (утвержден Приказом Минтруда от 15.09.2016 № 522н) **3.5.1. ТФ:** Обоснование необходимости защиты информации в автоматизированной системе **3.5.4. ТФ:** Моделирование защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации

- методами организации и управления деятельностью служб защиты информации на предприятии		
ОПК-6 «способностью применять приемы оказания первой помощи, методы и средства защиты персонала предприятия и населения в условиях чрезвычайных ситуаций, организовать мероприятия по охране труда и технике безопасности»		
Знать: - правовые основы, регулирующие будущую профессиональную деятельность обучающихся; - основные закономерности техногенного воздействия на окружающую среду; - самостоятельно методически правильно использовать средства и методы физического воспитания и самовоспитания для повышения адаптационных резервов организма, укрепления здоровья, коррекции физического развития и телосложения; - современную концепцию защиты объектов; Уметь: − предпринимать необходимые меры по восстановлению нарушенных прав; - организовывать мероприятия по охране и защите окружающей среды; - выбирать технические средства и технологии с учетом экологических последствий их применения; Владеть: - навыками критического восприятия информации;	Правоведение Основы управленческой деятельности Физическая культура Экология Технические средства охраны Технические средства безопасности Учебная практика	Профессиональный стандарт «Специалист по защите информации в автоматизированных системах» (утвержден Приказом Минтруда от 15.09.2016 № 522н) **3.2.2. ТФ:** Администрирование систем защиты информации автоматизированных систем **3.2.4. ТФ:** Обеспечение работоспособности систем защиты информации при возникновении нештатных ситуаций

- методами обеспечения безопасности людей и окружающей среды от вредных воздействий; - профессиональной терминологией.		
ОПК-7 «способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты»		
Знать: - основные термины по проблематике информационной безопасности; - компьютерную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности; - методологию создания систем защиты персональных данных при их обработке в компьютерных системах; - методологию создания систем менеджмента информационной безопасности; Уметь: − выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации; - разрабатывать предложения и организационно-распорядительные документы по защите персональных данных в организации и на предприятии; - оценивать информационные риски в корпоративных информационных системах; - разрабатывать предложения по совершенствованию системы управления информационной безопасностью	Основы информационной безопасности Программно-аппаратные средства защиты информации Криптографические методы защиты информации Техническая защита информации Безопасность жизнедеятельности Основы управления информационной безопасностью Информационные технологии Защита электронного документооборота Защита информационных процессов в компьютерных системах Безопасность систем баз данных Экология Экономика и финансы защиты информации Организация и управление службой защиты информации на предприятии Производственная практика Государственная итоговая аттестация	Профессиональный стандарт «Специалист по защите информации в автоматизированных системах» (утвержден Приказом Минтруда от 15.09.2016 № 522н) **3.2.5. ТФ:** Мониторинг защищенности информации в автоматизированных системах **3.3.2. ТФ:** Разработка организационно-распорядительных документов по защите информации в автоматизированных системах **3.3.3. ТФ:** Анализ уязвимостей внедряемой системы защиты информации **3.3.4. ТФ:** Внедрение организационных мер по защите информации в автоматизированных системах **3.4.2. ТФ:** Разработка проектных решений по защите информации в автоматизированных системах

Владеть: - навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем; - профессиональной терминологией в области обеспечения безопасности персональных данных; - методами мониторинга и аудита, выявления угроз и управления информационной безопасностью		
Эксплуатационная деятельность		
ПК-1 «способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации»		
Знать: - типовые средства и методы защиты информации в локальных и глобальных вычислительных сетях; - базовую конфигурацию системы защиты информации автоматизированной системы - особенности применения программных и программно-аппаратных средств защиты информации в автоматизированных системах; - типовые средства, методы и протоколы идентификации, аутентификации и авторизации; - технические средства контроля эффективности мер защиты информации; - содержание эксплуатационной документации автоматизированной системы; **Уметь:** - конфигурировать параметры системы защиты информации автоматизированной	Аппаратные средства вычислительной техники Программно-аппаратные средства защиты информации Криптографические методы защиты информации Техническая защита информации Безопасность жизнедеятельности Математические основы криптологии Технические средства охраны Технические средства безопасности Производственная практика	Профессиональный стандарт «Специалист по защите информации в автоматизированных системах» (утвержден Приказом Минтруда от 15.09.2016 № 522н) **3.1.1. ТФ:** Проведение регламентных работ по эксплуатации систем защиты информации автоматизированных систем **3.2.1. ТФ:** Диагностика систем защиты информации автоматизированных систем **3.3.1. ТФ:** Установка и настройка средств защиты информации в автоматизированных системах

системы в соответствии с ее эксплуатационной документацией; - обнаруживать и устранять неисправности системы защиты информации автоматизированной системы согласно эксплуатационной документации; - производить монтаж и диагностику компьютерных сетей; - использовать типовые криптографические средства защиты информации, в том числе средства электронной подписи; - определять источники и причины возникновения инцидентов; - устранять известные уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации; - определять параметры настройки программного обеспечения системы защиты информации автоматизированной системы; **Владеть (трудовые действия):** - проверка работоспособности системы защиты информации автоматизированной системы; - контроль соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации - контроль стабильности характеристик системы защиты информации автоматизированной системы; - обнаружение инцидентов в процессе эксплуатации автоматизированной системы		

- идентификация инцидентов в процессе эксплуатации автоматизированной системы; - входной контроль качества комплектующих изделий системы защиты информации автоматизированной системы; - осуществление автономной наладки технических и программных средств системы защиты информации автоматизированной системы; - проведение приемочных испытаний системы защиты информации автоматизированной системы; - внесение в эксплуатационную документацию изменений, направленных на устранение недостатков, выявленных в процессе испытаний.		
ПК-2 «способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач»		
Знать: - процедуры по архивированию информации, обрабатываемой автоматизированной системой; - назначение и принципы работы основных узлов современных технических средств информатизации; - регламент автоматизированной системы по уничтожению информации и машинных носителей информации; - содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем; **Уметь:**	Программно-аппаратные средства защиты информации Сети и системы передачи информации Языки программирования Технологии и методы программирования Информационные технологии Безопасность операционных систем Системное администрирование Сети и телекоммуникации Прикладное программирование Пакеты прикладных программ Системное программирование Производственная практика Государственная итоговая аттестация	Профессиональный стандарт «Специалист по защите информации в автоматизированных системах» (утвержден Приказом Минтруда от 15.09.2016 № 522н) **3.1.3. ТФ:** Обеспечение защиты информации при выводе из эксплуатации автоматизированных систем **3.2.4. ТФ:** Обеспечение работоспособности систем защиты информации при возникновении нештатных ситуаций

- использовать программные средства для архивирования информации; - использовать программные и программно-аппаратные средства для уничтожения информации и носителей информации; - использовать типовые криптографические средства защиты информации, в том числе электронную подпись; - применять типовые программные средства резервирования и восстановления информации в автоматизированных системах; - применять программные средства обеспечения безопасности данных; **Владеть (трудовые действия):** **- у**ничтожение информации, обрабатываемой автоматизированной системой; - архивирование информации, обрабатываемой автоматизированной системой; - резервирование программного обеспечения, технических средств, каналов передачи данных автоматизированной системы управления на случай возникновения нештатных ситуаций.		
ПК-3 «способностью администрировать подсистемы информационной безопасности объекта защиты»		
Знать: - принципы формирования политики информационной безопасности в автоматизированных системах; - программно-аппаратные средства защиты информации автоматизированных систем; - основные криптографические методы,	Системное администрирование Вычислительные сети Сетевая безопасность	Профессиональный стандарт «Специалист по защите информации в автоматизированных системах» (утвержден Приказом Минтруда от 15.09.2016 № 522н) **3.2.2. ТФ:** Администрирование систем защиты информации автоматизированных систем

алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах; - принципы организации и структура систем защиты программного обеспечения автоматизированных систем; - содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем безопасности автоматизированных систем; - методы контроля эффективности защиты информации от "утечки" по техническим каналам; **Уметь:** - создавать, удалять и изменять учетные записи пользователей автоматизированной системы; - устанавливать и настраивать операционные системы, системы управления базами данных, компьютерные сети и программные системы с учетом требований по обеспечению защиты информации; - регистрировать события, связанные с защитой информации в автоматизированных системах; - анализировать события, связанные с защитой информации в автоматизированных системах **Владеть (трудовые действия):** - установка обновлений программного обеспечения автоматизированной системы; - обеспечение безопасности информации с учетом требования эффективного		

функционирования автоматизированной системы; - управление полномочиями пользователей автоматизированной системы; - информирование пользователей о правилах эксплуатации автоматизированной системы с учетом требований по защите информации; - проведение занятий с персоналом по работе с системой защиты информации автоматизированной системы, включая проведение практических занятий с персоналом на макетах или в тестовой зоне.		
ПК-4 «способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты»		
Знать: - содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации; - основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; - нормативные правовые акты в области защиты информации; - руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; **Уметь:** - классифицировать и оценивать угрозы информационной безопасности; - применять нормативные документы по противодействию технической разведке;	Программно-аппаратные средства защиты информации Основы управления информационной безопасностью Методы оптимизации Методы вычислений Вычислительные сети Сетевая безопасность Преддипломная практика	Профессиональный стандарт «Специалист по защите информации в автоматизированных системах» (утвержден Приказом Минтруда от 15.09.2016 № 522н) **3.3.2. ТФ:** Разработка организационно-распорядительных документов по защите информации в автоматизированных системах

- контролировать эффективность принятых мер по защите информации в автоматизированных системах **Владеть (трудовые действия):** - определение правил и процедур управления системой защиты информации автоматизированной системы; - определение правил и процедур выявления инцидентов; - определение правил и процедур мониторинга обеспечения уровня защищенности информации автоматизированной системы; - определение правил и процедур защиты информации при выводе автоматизированной системы из эксплуатации; - определение правил и процедур реагирования на инциденты.		
ПК-5 «способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации»		
Знать: - основные методы и средства криптографической защиты информации; - способы защиты информации от "утечки" по техническим каналам; - способы контроля эффективности защиты информации от "утечки" по техническим каналам; - нормативные правовые акты в области защиты информации; - руководящие и методические документы уполномоченных федеральных органов	Информатика Криптографические методы защиты информации Сети и телекоммуникации Производственная практика	Профессиональный стандарт «Специалист по защите информации в автоматизированных системах» (утвержден Приказом Минтруда от 15.09.2016 № 522н) **3.3.3. ТФ:** Анализ уязвимостей внедряемой системы защиты информации

исполнительной власти по защите информации **Уметь:** - классифицировать и оценивать угрозы безопасности информации автоматизированной системы; - разрабатывать предложения по совершенствованию системы управления защитой информации автоматизированной системы; - проводить анализ доступных информационных источников с целью выявления известных уязвимостей используемых в системе защиты информации программных и программно-аппаратных средств; **Владеть (трудовые действия):** - проведение анализа уязвимости программных и программно-аппаратных средств системы защиты информации автоматизированной системы; - проведение экспертизы состояния защищенности информации автоматизированных систем; - уточнение модели угроз безопасности информации автоматизированной системы; - проведение анализа уязвимостей автоматизированных и информационных систем.		
ПК-6 «способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации»		
Знать: - нормативные правовые акты и	Техническая защита информации Безопасность жизнедеятельности	Профессиональный стандарт

национальные стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации; - руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; - организационные меры по защите информации; - методики сертификационных испытаний технических средств защиты информации от "утечки" по техническим каналам на соответствие требованиям по безопасности информации; **Уметь:** - обучать персонал автоматизированной системы комплексу мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения защиты информации; - осуществлять планирование и организацию работы персонала автоматизированной системы с учетом требований по защите информации; - реализовывать правила разграничения доступа персонала к объектам доступа; **Владеть (трудовые действия):** - проведение проверки полноты описания в организационно-распорядительных документах на автоматизированную систему действий персонала по реализации организационных мер защиты информации;	Безопасность операционных систем Системное администрирование Прикладное программирование Пакеты прикладных программ Системное программирование Производственная практика	«Специалист по защите информации в автоматизированных системах» (утвержден Приказом Минтруда от 15.09.2016 № 522н) **3.3.4. ТФ:** Внедрение организационных мер по защите информации в автоматизированных системах

- проведение занятий с персоналом по работе с системой защиты информации автоматизированной системы, включая проведение практических занятий на макетах или в тестовой зоне; - проведение проверки готовности персонала к эксплуатации системы защиты информации автоматизированной системы; - подготовка документов, определяющих правила и процедуры контроля обеспеченности уровня защищенности информации, содержащейся в информационной системе; - подготовка документов, определяющих правила и процедуры выявления инцидентов, которые могут привести к сбоям или нарушению функционирования информационной системы и возникновению угроз безопасности информации.		
Проектно-технологическая деятельность		
ПК-7 «способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений»		
Знать: - нормативные правовые акты и национальные стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации; - принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей и их компонентов; - особенности защиты информации в	Сети и системы передачи информации Технологии и методы программирования Основы управления информационной безопасностью Комплексные системы защиты информации на предприятии Пакеты прикладных программ Системное программирование Среда моделирования Компьютерная графика Вычислительные сети	Профессиональный стандарт «Специалист по защите информации в автоматизированных системах» (утвержден Приказом Минтруда от 15.09.2016 № 522н) **3.4.2. ТФ:** Разработка проектных решений по защите информации в автоматизированных системах

автоматизированных системах управления технологическими процессами; - критерии оценки эффективности и надежности средств защиты информации программного обеспечения автоматизированных систем; - принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем; - принципы формирования политики информационной безопасности в автоматизированных системах; **Уметь:** - применять действующую нормативную базу в области обеспечения защиты информации; - применять нормативные документы по противодействию технической разведке; - определять типы субъектов доступа и объектов доступа, являющихся объектами защиты; - определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в автоматизированной системе; - выбирать меры защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы; - определять виды и типы средств защиты информации, обеспечивающих реализацию технических мер защиты информации; - определять структуру системы защиты информации автоматизированной системы в	Сетевая безопасность Производственная практика Преддипломная практика Государственная итоговая аттестация	

соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем; **Владеть (трудовые действия):** - разработка модели угроз безопасности информации и модели нарушителя в автоматизированных системах; - разработка моделей автоматизированных систем и подсистем безопасности автоматизированных систем; - разработка проектов нормативных документов, регламентирующих работу по защите информации; - разработка предложений по совершенствованию системы управления безопасностью информации в автоматизированных системах.		
ПК-8 «способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов»		
Знать: - национальные, межгосударственные и международные стандарты в области защиты информации; - основные меры по защите информации в автоматизированных системах; - особенности защиты информации в автоматизированных системах управления технологическими процессами; - угрозы безопасности, информационные воздействия, критерии оценки защищенности и методы защиты информации в автоматизированных системах; - методы, способы, средства,	Документоведение Метрология и электрорадиоизмерения Системное администрирование Производственная практика	Профессиональный стандарт «Специалист по защите информации в автоматизированных системах» (утвержден Приказом Минтруда от 15.09.2016 № 522н) **3.4.3. ТФ:** Разработка эксплуатационной документации на системы защиты информации автоматизированных систем

последовательность и содержание этапов разработки автоматизированных систем и систем защиты информации автоматизированных системах; - программно-аппаратные средства обеспечения защиты информации в программном обеспечении автоматизированных систем; **Уметь:** - определять меры (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации в автоматизированных системах; - разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем; - проектировать подсистемы безопасности информации с учетом действующих нормативных и методических документов; - анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей систем защиты информации автоматизированных систем; - проводить технико-экономическое обоснование проектных решений программно-аппаратных средств обеспечения защиты информации в автоматизированной системе с целью обеспечения требуемого уровня		

защищенности; - проводить комплексное тестирование и отладку аппаратных и программных систем защиты информации; **Владеть (трудовые действия):** - анализ технической документации информационной инфраструктуры автоматизированной системы; - анализ защищенности информационной инфраструктуры автоматизированной системы; - формирование требований по защите информации, включая использование математического аппарата для решения прикладных задач; - документирование программного обеспечения, технических средств, баз данных и компьютерных сетей с учетом требований по обеспечению защиты информации.		
Экспериментально-исследовательская деятельность		
ПК-9 «способностью осуществлять подбор, изучение и обобщение научно- технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности»		
Знать: - принципы формирования политики информационной безопасности в автоматизированных системах; - нормативные правовые акты в области защиты информации; - национальные, межгосударственные и международные стандарты в области защиты информации;	Основы управления информационной безопасностью Защита электронного документооборота Комплексные системы защиты информации на предприятии Технический иностранный язык Теория принятия решений Автоматизированные системы обработки информации и управления	Профессиональный стандарт «Специалист по защите информации в автоматизированных системах» (утвержден Приказом Минтруда от 15.09.2016 № 522н) **3.5.1. ТФ:** Обоснование необходимости защиты информации в автоматизированной системе

- руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; - организационные меры по защите информации; - методики сертификационных испытаний технических средств защиты информации от "утечки" по техническим каналам на соответствие требованиям по безопасности информации; - содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации; **Уметь:** - анализировать цели создания автоматизированных систем и задачи, решаемые автоматизированными системами; - классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности и оценивать угрозы безопасности информации; - определять класс защищенности автоматизированных систем и ее составных частей; **Владеть (трудовые действия):** - анализ характера обрабатываемой информации и определение перечня информации, подлежащей защите; - определение требуемого класса (уровня) защищенности автоматизированной системы;	Преддипломная практика Государственная итоговая аттестация	

- обоснование необходимости использования криптографических средств защиты информации; - разработка отчетных документов и разделов технических заданий.		
ПК-10 «способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности»		
Знать: - **о**сновные угрозы безопасности информации и модели нарушителя в автоматизированных системах; - основные методы и средства криптографической защиты информации; - способы защиты информации от "утечки" по техническим каналам; - принципы построения и функционирования систем и сетей передачи информации - эталонную модель взаимодействия открытых систем; - основные информационные технологии, используемые в автоматизированных системах; - виды информационных воздействий и критерии оценки защищенности информации в автоматизированных системах; - основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в вычислительных сетях; - способы реализации угроз безопасности в автоматизированных системах; **Уметь:**	Защита и обработка конфиденциальных документов Безопасность операционных систем Защита информационных процессов в компьютерных системах Комплексные системы защиты информации на предприятии Преддипломная практика	Профессиональный стандарт «Специалист по защите информации в автоматизированных системах» (утвержден Приказом Минтруда от 15.09.2016 № 522н) **3.2.5. ТФ:** Мониторинг защищенности информации в автоматизированных системах **3.3.3. ТФ:** Анализ уязвимостей внедряемой системы защиты информации **3.4.1. ТФ:** Тестирование систем защиты информации автоматизированных систем **3.5.1. ТФ**: Обоснование необходимости защиты информации в автоматизированной системе **3.5.2. ТФ:** Определение угроз безопасности информации, обрабатываемой автоматизированной системой

- анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах; - проводить анализ доступных информационных источников с целью выявления известных уязвимостей используемых в системе защиты информации программных и программно-аппаратных средств; - классифицировать и оценивать угрозы безопасности информации автоматизированной системы; - анализировать основные характеристики и возможности телекоммуникационных систем по передаче информации; - анализировать основные узлы и устройства современных автоматизированных систем; - анализировать цели создания автоматизированных систем и задачи, решаемые автоматизированными системами; - выявлять уязвимости информационно-технологических ресурсов автоматизированных систем; - классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности и оценивать угрозы безопасности информации; - анализировать возможные уязвимости		

информационных систем; - выявлять известные уязвимости информационных систем; **Владеть (трудовые действия):** - анализ недостатков в функционировании системы защиты информации автоматизированной системы; - выработка рекомендаций для принятия решения о модернизации системы защиты информации автоматизированной системы; - проведение анализа уязвимости программных и программно-аппаратных средств системы защиты информации автоматизированной системы; - проведение экспертизы состояния защищенности информации автоматизированных систем; - проведение анализа уязвимостей автоматизированных и информационных систем; - проведение анализа структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем; - выявление уязвимости информационно-технологических ресурсов автоматизированных систем; - выявление основных угроз безопасности информации в автоматизированных системах;		

- анализ характера обрабатываемой информации и определение перечня информации, подлежащей защите; - выявление степени участия персонала в обработке защищаемой информации - обоснование необходимости использования криптографических средств защиты информации; - определение оценки возможностей внешних и внутренних нарушителей; - анализ требований к назначению, структуре и конфигурации создаваемой автоматизированной системы с целью выявления угроз безопасности информации; - определение структурно-функциональных характеристик информационной системы в соответствии с требованиями нормативных правовых документов в области защиты информации.		
ПК-11 «способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов»		
Знать: - национальные, межгосударственные и международные стандарты в области защиты информации; - руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; - критерии оценки защищенности автоматизированной системы; - регламент информирования персонала автоматизированной системы о выявленных инцидентах	Технологии и методы программирования Метрология и электрорадиоизмерения Производственная практика	Профессиональный стандарт «Специалист по защите информации в автоматизированных системах» (утвержден Приказом Минтруда от 15.09.2016 № 522н) **3.2.1. ТФ:** Диагностика систем защиты информации автоматизированных систем **3.4.1. ТФ:** Тестирование систем защиты информации автоматизированных систем; **3.5.4. ТФ:** Моделирование защищенных автоматизированных систем с целью анализа

- регламент учета выявленных инцидентов; - основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения защиты информации в автоматизированных системах; - основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; - организацию защиты информации от "утечки" по техническим каналам на объектах информатизации; - методы и технологии проектирования, моделирования, исследования систем защиты информации автоматизированных систем; **Уметь:** - определять источники и причины возникновения инцидентов; - оценивать последствия выявленных инцидентов; - обнаруживать нарушения правил разграничения доступа; - осуществлять контроль обеспечения уровня защищенности в автоматизированных системах; - анализировать основные узлы и устройства современных автоматизированных систем; - применять действующую нормативную базу в области обеспечения безопасности информации; - разрабатывать и исследовать математические модели конкретных		их уязвимостей и эффективности средств и способов защиты информации

явлений и процессов для решения расчетных и исследовательских задач; - применять математические модели при проектировании систем защиты информации автоматизированных систем; **Владеть (трудовые действия):** - обнаружение инцидентов в процессе эксплуатации автоматизированной системы - идентификация инцидентов в процессе; эксплуатации автоматизированной системы; - оценка защищенности автоматизированных систем с помощью типовых программных средств; - подбор инструментальных средств тестирования систем защиты информации автоматизированных систем; - составление протоколов тестирования систем защиты информации автоматизированных систем; - разработка модели угроз безопасности информации и нарушителей в автоматизированных системах; - исследование программных, архитектурно-технических и схемотехнических решений компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах; - анализ информационной инфраструктуры и безопасности информации автоматизированных систем.		
ПК-12 «способностью принимать участие в проведении экспериментальных исследований системы защиты информации»		

Знать: - основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; - основные меры по защите информации в автоматизированных системах; - особенности защиты информации в автоматизированных системах управления технологическими процессами; - принципы формирования политики информационной безопасности в автоматизированных системах; - нормативные правовые акты в области защиты информации; - руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; - организационные меры по защите информации; **Уметь:** - применять действующую нормативную базу в области обеспечения безопасности информации; - контролировать безотказное функционирование технических средств защиты информации; - организовывать работы по созданию, внедрению, проектированию, разработке и сопровождению защищенных автоматизированных систем;	Защита и обработка конфиденциальных документов Безопасность систем баз данных Сети и телекоммуникации Производственная практика	Профессиональный стандарт «Специалист по защите информации в автоматизированных системах» (утвержден Приказом Минтруда от 15.09.2016 № 522н) **3.4.1. ТФ:** Тестирование систем защиты информации автоматизированных систем **3.5.1. ТФ**: Обоснование необходимости защиты информации в автоматизированной системе

- использовать рисковую методологию управления защитой информации в автоматизированной системе; **Владеть (трудовые действия):** - составление протоколов тестирования систем защиты информации автоматизированных систем; - планирование мероприятий по обеспечению защиты информации в автоматизированной системе; - разработка отчетных документов и разделов технических заданий		
Организационно-управленческая деятельность		
ПК-13 «способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации»		
Знать: - основные методические и руководящие документы уполномоченных федеральных органов исполнительной власти по защите информации; - эксплуатационную и проектную документацию на автоматизированную систему; - основные методы управления защитой информации; - основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; - содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации;	Защита электронного документооборота Защита информационных процессов в компьютерных системах Комплексные системы защиты информации на предприятии Преддипломная практика	Профессиональный стандарт «Специалист по защите информации в автоматизированных системах» (утвержден Приказом Минтруда от 15.09.2016 № 522н) **3.1.2. ТФ:** Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем **3.2.3. ТФ:** Управление защитой информации в автоматизированных системах **3.3.2 ТФ:** Разработка организационно-распорядительных документов по защите информации в автоматизированных системах **3.3.4. ТФ:**

- основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; - организационные меры по защите информации; **Уметь:** - оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации; - определять подлежащие защите информационные ресурсы автоматизированных систем; - применять нормативные документы по противодействию технической разведке; - контролировать эффективность принятых мер по защите информации в автоматизированных системах; - обучать персонал автоматизированной системы комплексу мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения защиты информации; **Владеть (трудовые действия):** - ведение документов учета, обработки, хранения и передачи информации, составляющей тайну; - ведение протоколов и журналов учета при изменении конфигурации систем защиты информации автоматизированных систем; - ведение протоколов и журналов учета при осуществлении мониторинга систем защиты информации автоматизированных систем;		Внедрение организационных мер по защите информации в автоматизированных системах

- составление комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе; - определение правил и процедур управления системой защиты информации автоматизированной системы; - определение правил и процедур мониторинга обеспечения уровня защищенности информации автоматизированной системы; - проведение проверки полноты описания в организационно-распорядительных документах на автоматизированную систему действий персонала по реализации организационных мер защиты информации; - подготовка документов, определяющих правила и процедуры выявления инцидентов, которые могут привести к сбоям или нарушению функционирования информационной системы и возникновению угроз безопасности информации.		
ПК-14 «способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности»		
Знать: - организационные меры по защите информации; - содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем; - организационные меры по защите информации;	Защита и обработка конфиденциальных документов Безопасность систем баз данных Структуры и основы деятельности предприятий различных форм собственности Экономика и финансы защиты информации Организация и управление службой защиты информации на предприятии Преддипломная практика	Профессиональный стандарт «Специалист по защите информации в автоматизированных системах» (утвержден Приказом Минтруда от 15.09.2016 № 522н) **3.2.1. ТФ:** Диагностика систем защиты информации автоматизированных систем **3.2.4. ТФ:**

- руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; - организационные меры по защите информации; **Уметь:** - обнаруживать нарушения правил разграничения доступа; - устранять нарушения правил разграничения доступа; - документировать действия по устранению неисправностей в работе системы защиты информации автоматизированной системы; - обучать персонал автоматизированной системы комплексу мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения защиты информации; - осуществлять планирование и организацию работы персонала автоматизированной системы с учетом требований по защите информации; **Владеть (трудовые действия):** - расчет показателей эффективности защиты информации, обрабатываемой в автоматизированных системах; - проведение занятий с персоналом по работе с системой защиты информации автоматизированной системы, включая проведение практических занятий на макетах или в тестовой зоне;		Обеспечение работоспособности систем защиты информации при возникновении нештатных ситуаций **3.3.4. ТФ:** Внедрение организационных мер по защите информации в автоматизированных системах

- подготовка документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации; - проведение проверки готовности персонала к эксплуатации системы защиты информации автоматизированной системы; - подготовка документов, определяющих правила и процедуры контроля обеспеченности уровня защищенности информации, содержащейся в информационной системе.		
ПК-15 «способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю»		
Знать: - назначение и принципы работы основных узлов современных технических средств информатизации; - организацию ремонтного обслуживания компонентов автоматизированной системы; - регламент автоматизированной системы по уничтожению информации и машинных носителей информации; - основные методы управления защитой информации; - основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; - содержание и порядок деятельности персонала по эксплуатации защищенных	Защита и обработка конфиденциальных документов Защита информационных процессов в компьютерных системах Прикладное программирование Преддипломная практика Государственная итоговая аттестация	Профессиональный стандарт «Специалист по защите информации в автоматизированных системах» (утвержден Приказом Минтруда от 15.09.2016 № 522н) **3.1.3. ТФ:** Обеспечение защиты информации при выводе из эксплуатации автоматизированных систем **3.2.3. ТФ:** Управление защитой информации в автоматизированных системах **3.3.2. ТФ:** Разработка организационно-распорядительных документов по защите информации в автоматизированных системах

автоматизированных систем и систем защиты информации; - основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; - руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; **Уметь:** - использовать программные и программно-аппаратные средства для уничтожения информации и носителей информации; - использовать типовые криптографические средства защиты информации, в том числе электронную подпись; - разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем; - применять технические средства контроля эффективности мер защиты информации; - контролировать эффективность принятых мер по защите информации в автоматизированных системах; **Владеть (трудовые действия):** - архивирование информации, обрабатываемой автоматизированной системой; - составление комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе;		

- определение правил и процедур управления системой защиты информации автоматизированной системы; - определение правил и процедур выявления инцидентов; - определение правил и процедур мониторинга обеспечения уровня защищенности информации автоматизированной системы.		