

**ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ «АНАЛИЗ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ»
ПО СПЕЦИАЛЬНОСТИ 10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ**

**область профессиональной деятельности и (или) сферы профессиональной деятельности, в которых выпускники ОПОП могут осуществлять профессиональную деятельность – обеспечение безопасности (в сфере обеспечения безопасности информации в автоматизированных системах, обладающих информационно-технологическими ресурсами, подлежащими защите)
тип задач профессиональной деятельности – - проектный; - контрольно-аналитический**

задачи профессиональной деятельности:

- 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;
- 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;
- контроль работоспособности и эффективности применяемых средств защиты информации;
- организация работ по созданию, внедрению, эксплуатации и сопровождению защищенных автоматизированных систем;
- администрирование подсистем информационной безопасности автоматизированных систем;
- разработка и исследование моделей информационно-технологических ресурсов, модели угроз и модели нарушителей информационной безопасности в распределенных информационных системах;
- аудит защищенности информационно-технологических ресурсов;
- координация деятельности подразделений и специалистов по защите информации в организациях, в том числе на предприятиях и в учреждениях;

основание для определения профессиональных компетенций и практической подготовки:

- Профессиональный стандарт 06.033 «СПЕЦИАЛИСТ ПО ЗАЩИТЕ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ».
- Обобщенная трудовая функция: D. Формирование требований к защите информации в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости

УНИВЕРСАЛЬНЫЕ КОМПЕТЕНЦИИ (УК)

<i>Категория (группа) УК</i>	<i>Код и наименование УК</i>	<i>Код и наименование индикатора достижения УК</i>	<i>Дисциплины / практики, участвующие в формировании УК</i>	<i>Воспитательная работа / практическая подготовка</i>	<i>Направление воспитательной работы / практической подготовки</i>
Системное и критическое мышление	УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, выработать стратегию действий	УК-1.1 Знает метод системного анализа, способы обоснования решения (индукция, дедукция, по аналогии) проблемной ситуации УК-1.2 Умеет применять методики поиска, сбора и обработки информации; осуществляет оценку адекватности информации о проблемной ситуации путём выявления диалектических и формально-логических противоречий в анализируемой информации УК-1.3 Владеет методами поиска, сбора и обработки, критического анализа и синтеза информации; навыком выбора методов критического анализа, адекватных проблемной ситуации; навыками разработки и обоснования плана действий по решению проблемной ситуации	Введение в профессиональную деятельность		
			Философия		
			Производственная практика (преддипломная практика)		
			Производственная практика (научно-исследовательская работа)		
Разработка и реализация проектов	УК-2 Способен управлять проектом на всех этапах его жизненного цикла	УК-2.1 Знает виды ресурсов и ограничений для реализации проекта; основные методы оценки разных способов решения задач; действующее законодательство и правовые нормы, регулирующие профессиональную деятельность УК-2.2 Формулирует цели, задачи, ожидаемые результаты проекта;	Экономика		
			Правоведение		
			Технологии создания StartUp (факультатив)		

<i>Категория (группа) УК</i>	<i>Код и наименование УК</i>	<i>Код и наименование индикатора достижения УК</i>	<i>Дисциплины / практики, участвующие в формировании УК</i>	<i>Воспитательная работа / практическая подготовка</i>	<i>Направление воспитательной работы / практической подготовки</i>
		разрабатывает план реализации проекта; использует нормативно-правовую документацию в сфере профессиональной деятельности УК-2.3 Владеет методиками разработки цели и задач проекта; методами оценки потребности в ресурсах, продолжительности и стоимости проекта; навыками работы с нормативно-правовой документацией; навыками контроля и оценки эффективности реализации			
Командная работа и лидерство	УК-3 Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	УК-3.1 Знает основные приемы и нормы социального взаимодействия; основные понятия и методы конфликтологии, технологии межличностной и деловой коммуникации, принципы командной работы как основы организации и руководства работой команды, способы мотивации членов команды с учетом организационных возможностей и личностных особенностей членов команды УК-3.2 Умеет устанавливать и поддерживать контакты, обеспечивающие успешную работу в команде; разрабатывать цели команды в соответствии с целями проекта; выбирать стратегию формирования	Руководство и управление службой безопасности		
			Б1.В.ДВ.01.01 Теория и практика успешной коммуникации		
			Б1.В.ДВ.01.02 Социально-психологические аспекты инклюзивного образования		

<i>Категория (группа) УК</i>	<i>Код и наименование УК</i>	<i>Код и наименование индикатора достижения УК</i>	<i>Дисциплины / практики, участвующие в формировании УК</i>	<i>Воспитательная работа / практическая подготовка</i>	<i>Направление воспитательной работы / практической подготовки</i>
		команды и определять функциональные и ролевые критерии отбора участников УК-3.3 Имеет навыки организации и руководства работой команды, презентации результатов собственной и командной работы			
Коммуникация	УК-4 Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	<p>УК-4.1 Знает методики поиска, сбора и обработки информации с помощью информационно-коммуникационных технологий; актуальные российские и зарубежные источники информации в сфере профессиональной деятельности; особенности устного и письменного общения на русском и иностранном языках; правила и закономерности деловой устной и письменной коммуникации</p> <p>УК-4.2 Умеет применять различные методы делового общения на русском и иностранном языках как в устной, так и в письменной форме; представляет информацию на русском и иностранном языке с помощью информационно-коммуникационных технологий</p> <p>УК-4.3 Владеет навыками чтения и перевода текстов на иностранном языке в профессиональном общении; навыками деловых коммуникаций в устной и письменной форме на русском и</p>	Русский язык и культура речи		
			Иностранный язык		

<i>Категория (группа) УК</i>	<i>Код и наименование УК</i>	<i>Код и наименование индикатора достижения УК</i>	<i>Дисциплины / практики, участвующие в формировании УК</i>	<i>Воспитательная работа / практическая подготовка</i>	<i>Направление воспитательной работы / практической подготовки</i>
		иностранных языках			
Межкультурное взаимодействие	УК-5 Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	<p>УК-5.1 Знает особенности взаимоотношений в системе «мир – человек»; основные этапы развития России; особенности современной политической организации российского общества; фундаментальные достижения, связанные с развитием русской земли и российской цивилизации; способы и средства эффективного взаимодействия в социуме и выражения (демонстрации) гражданской позиции</p> <p>УК-5.2 Умеет адекватно воспринимать актуальные социальные и культурные различия, уважительно и бережно относиться к историческому наследию и культурным традициям России, как части мирового наследия</p> <p>УК-5.3 Владеет навыками осознанного выбора ценностных ориентиров и гражданской позиции; навыками аргументированного обсуждения и решения проблем мировоззренческого, общественного и личностного характера; навыками самостоятельного критического мышления</p>	Основы российской государственности		
			Б1.В.ДВ.01.01 Теория и практика успешной коммуникации		
			Б1.В.ДВ.01.02 Социально-психологические аспекты инклюзивного образования		
			История России		
			Философия		

<i>Категория (группа) УК</i>	<i>Код и наименование УК</i>	<i>Код и наименование индикатора достижения УК</i>	<i>Дисциплины / практики, участвующие в формировании УК</i>	<i>Воспитательная работа / практическая подготовка</i>	<i>Направление воспитательной работы / практической подготовки</i>
Самоорганизация и саморазвитие (в том числе здоровьесбережение)	УК-6 Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни	УК-6.1 Знает основные принципы самовоспитания и самообразования, профессионального и личного развития, исходя из этапов карьерного роста и требований рынка труда УК-6.2 Формулирует цели личного и профессионального развития и условия их достижения, исходя из индивидуально-личностных особенностей, поставленных жизненных целей и развития социальной ситуации УК-6.3 Владеет технологиями приобретения, использования и обновления социокультурных и профессиональных знаний, умений и навыков; методиками саморазвития и самообразования	Введение в профессиональную деятельность		
			Б1.В.ДВ.01.01 Теория и практика успешной коммуникации		
			Б1.В.ДВ.01.02 Социально-психологические аспекты инклюзивного образования		
Самоорганизация и саморазвитие (в том числе здоровьесбережение)	УК-7 Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности	УК-7.1 Знает роль и значение физической культуры в жизни человека и общества; научно-практические основы физической культуры, а также систему профилактики вредных привычек и формирования здорового образа и стиля жизни УК-7.2 Умеет применять на практике разнообразные средства физической культуры и спорта для сохранения и укрепления здоровья и психофизической подготовки; использует средства и	Тайм-менеджмент (факультатив)		
			Физическая культура и спорт		
			Б1.О.ДВ.03.01 Прикладная физическая культура		
			Б1.О.ДВ.03.02 Спортивные и подвижные игры		
			Б1.О.ДВ.03.03 Фитнес-культура		

<i>Категория (группа) УК</i>	<i>Код и наименование УК</i>	<i>Код и наименование индикатора достижения УК</i>	<i>Дисциплины / практики, участвующие в формировании УК</i>	<i>Воспитательная работа / практическая подготовка</i>	<i>Направление воспитательной работы / практической подготовки</i>
		методы физического воспитания для профессионально-личностного развития, физического самосовершенствования, формирования здорового образа и стиля жизни УК-7.3 Владеет навыками поддержания здоровья и физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности			
Безопасность жизнедеятельности	УК-8 Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных	УК-8.1 Знает классификацию и источники чрезвычайных ситуаций природного и техногенного происхождения; причины, признаки и последствия опасностей, методы защиты в условиях чрезвычайных ситуаций, военных конфликтов; принципы организации безопасности труда на предприятии, технические средства защиты людей в условиях чрезвычайной ситуации, методы сохранения природной среды, факторы обеспечения устойчивого развития общества УК-8.2 Умеет поддерживать безопасные условия жизнедеятельности; обеспечивать условия труда на рабочем месте; выявлять признаки, причины и условия возникновения чрезвычайных ситуаций; оценивать вероятность	Основы военной подготовки		
			Безопасность жизнедеятельности		
			Учебная практика (учебно-лабораторный практикум)		

<i>Категория (группа) УК</i>	<i>Код и наименование УК</i>	<i>Код и наименование индикатора достижения УК</i>	<i>Дисциплины / практики, участвующие в формировании УК</i>	<i>Воспитательная работа / практическая подготовка</i>	<i>Направление воспитательной работы / практической подготовки</i>
	ситуаций и военных конфликтов	возникновения потенциальной опасности и принимать меры по ее предупреждению УК-8.3 Владеет методами прогнозирования возникновения опасных или чрезвычайных ситуаций; навыками по применению основных методов защиты в условиях чрезвычайных ситуаций			
Экономическая культура, в том числе финансовая грамотность	УК-9 Способен принимать обоснованные экономические решения в различных областях жизнедеятельности	УК-9.1 Знает базовые принципы функционирования экономики и экономического развития, цели и формы участия государства в экономике, методы личного экономического и финансового планирования, основные финансовые инструменты, используемые для управления личными финансами УК-9.2 Умеет анализировать информацию для принятия обоснованных экономических решений, применять экономические знания при выполнении практических задач УК-9.3 Владеет способностью использовать основные положения и методы экономических наук при решении социальных и профессиональных задач	Экономика		

<i>Категория (группа) УК</i>	<i>Код и наименование УК</i>	<i>Код и наименование индикатора достижения УК</i>	<i>Дисциплины / практики, участвующие в формировании УК</i>	<i>Воспитательная работа / практическая подготовка</i>	<i>Направление воспитательной работы / практической подготовки</i>
Гражданская позиция	УК-10 Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	УК-10.1 Знает сущность, причины, разновидности экстремизма и терроризма; сущность коррупционного поведения и его взаимосвязь с социальными, экономическими, политическими и иными условиями; нормативно-правовые акты в сфере противодействия экстремизму, терроризму, коррупции	Противодействие экстремизму, терроризму, коррупции		
		УК-10.2 Умеет выявлять признаки экстремизма и терроризма в различных информационных материалах; формулировать требования к антитеррористической защищенности объектов; анализировать; толковать и применять правовые нормы о противодействии экстремизму, терроризму, коррупционному поведению УК-10.3 Владеет навыками выявления причин, способствующих совершению преступлений экстремистской, террористической и коррупционной направленности, в том числе в профессиональной деятельности	Учебная практика (ознакомительная практика)		

ОБЩЕПРОФЕССИОНАЛЬНЫЕ КОМПЕТЕНЦИИ (ОПК)

<i>Категория (группа) ОПК (при наличии)</i>	<i>Код и наименование ОПК</i>	<i>Код и наименование индикатора достижения ОПК</i>	<i>Дисциплины / практики, участвующие в формировании ОПК</i>	<i>Практическая подготовка</i>	<i>Трудовая функция</i>
	ОПК-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;	<p>ОПК-1.1 Знает понятие информационного общества, его характерные черты и признаки, основные тенденции развития; сущность информационной инфраструктуры; основные формы проявления информации, её свойства как объекта безопасности; угрозы и источники угроз информационной безопасности современного общества</p> <p>ОПК-1.2 Умеет выполнять поиск и анализ информации для принятия решений; умеет применять основные методы обеспечения информационной безопасности</p> <p>ОПК-1.3 Владеет навыками работы с компьютером как средством управления информацией; навыками использования облачных технологий для хранения и обработки информации; навыками защиты конфиденциальности и данных во всех объектах сетевой инфраструктуры, онлайн-приложениях и платформах</p>	Информационные технологии		
			Основы информационной безопасности		
			Учебная практика (ознакомительная практика)		
	ОПК-2 Способен применять программные средства системного и прикладного назначения, в том числе	ОПК-2.1 Знает теорию в области использования современных языков и систем программирования, особенности функционирования программных средств системного и прикладного назначений	Современные программные средства		
			Операционные системы		
			Базы данных		
			Альтернативные		

<i>Категория (группа) ОПК (при наличии)</i>	<i>Код и наименование ОПК</i>	<i>Код и наименование индикатора достижения ОПК</i>	<i>Дисциплины / практики, участвующие в формировании ОПК</i>	<i>Практическая подготовка</i>	<i>Трудовая функция</i>
	отечественного производства, для решения задач профессиональной деятельности;	ОПК-2.2 Умеет разрабатывать оконные приложения, рационально использовать функциональные возможности программных средств системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности ОПК-2.3 Владеет навыками разработки приложений с использованием WinAPI; использования системного программного обеспечения для решения задач профессиональной деятельности	операционные системы		
Учебная практика (учебно-лабораторный практикум)					
Технологии создания и продвижения сайтов (факультатив)					
	ОПК-3 Способен использовать математические методы, необходимые для решения задач профессиональной деятельности;	ОПК-3.1 Знает математические методы, необходимые для решения задач профессиональной деятельности ОПК-3.2 Умеет использовать типовые математические методы и модели для решения задач профессиональной деятельности ОПК-3.3 Владеет навыками решения стандартных математических задач, выполнения расчетов математических величин, применения математических методов для решения задач профессиональной деятельности	Математический анализ		
Линейная алгебра и аналитическая геометрия					
Дискретная математика					
Теория вероятностей и математическая статистика					
Математическая логика и теория алгоритмов					
	ОПК-4 Способен анализировать фи-	ОПК-4.1 Знает основные понятия, законы и модели физики, основные фи-	Физика		
			Электроника и схе-		

<i>Категория (группа) ОПК (при наличии)</i>	<i>Код и наименование ОПК</i>	<i>Код и наименование индикатора достижения ОПК</i>	<i>Дисциплины / практики, участвующие в формировании ОПК</i>	<i>Практическая подготовка</i>	<i>Трудовая функция</i>
	зическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности;	зические явления, основные каналы утечки информации за счет существования физических полей; принципы работы элементов и функциональных узлов электронной аппаратуры, типовые схемотехнические решения основных узлов и блоков электронной аппаратуры ОПК-4.2 Умеет использовать физические законы, анализировать и применять модели явлений, процессов и объектов (включая схемы электронных устройств) при решении инженерных задач в профессиональной деятельности; проводить измерения и оценку параметров сигналов в информационных системах ОПК-4.3 Владеет основными методами теоретического и экспериментального исследования физических явлений и процессов, в том числе лежащих в основе микроэлектронной техники; навыками разработки и оптимизация электронных схем с учетом требований по защите информации	мотехника Измерение и оценка параметров сигналов в распределенных информационных системах Защита информации от утечки по техническим каналам		
	ОПК-5 Способен применять нормативные правовые акты, нормативные и методические до-	ОПК-5.1 Знает основные нормативные правовые акты в области защиты информации; национальные, межгосударственные и международные стандарты в области защиты инфор-	Организационное и правовое обеспечение информационной безопасности Производственная		

<i>Категория (группа) ОПК (при наличии)</i>	<i>Код и наименование ОПК</i>	<i>Код и наименование индикатора достижения ОПК</i>	<i>Дисциплины / практики, участвующие в формировании ОПК</i>	<i>Практическая подготовка</i>	<i>Трудовая функция</i>
	кументы, регламентирующие деятельность по защите информации;	<p>мации</p> <p>ОПК-5.2 Умеет находить необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с помощью правовых информационных систем; применять действующую законодательную базу в области информационной безопасности; разрабатывать проекты нормативных документов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов</p> <p>ОПК-5.3 Владеет навыками использования нормативных актов в профессиональной деятельности</p>	практика (преддипломная практика)		
	ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и ме-	<p>ОПК-6.1 Знает основные нормативные правовые акты, нормативные и методические документы ФСБ, ФСТЭК в области защиты информации ограниченного доступа</p> <p>ОПК-6.2 Умеет применять на практике основные нормативные правовые акты, нормативные и методические документы ФСБ, ФСТЭК в области защиты информации ограниченного доступа</p> <p>ОПК-6.3 Владеет навыками использо-</p>	<p>Организация и технология защиты конфиденциальной информации в информационных системах</p> <p>Организация и технология защиты информации в распределенных информационных системах</p> <p>Разработка политики</p>		

<i>Категория (группа) ОПК (при наличии)</i>	<i>Код и наименование ОПК</i>	<i>Код и наименование индикатора достижения ОПК</i>	<i>Дисциплины / практики, участвующие в формировании ОПК</i>	<i>Практическая подготовка</i>	<i>Трудовая функция</i>
	<p>тодическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;</p>	<p>вания нормативных правовых актов, нормативных и методических документов ФСБ, ФСТЭК в области защиты информации ограниченного доступа при решении профессиональных задач</p>	информационной безопасности		
			Производственная практика (преддипломная практика)		
	<p>ОПК-7 Способен создавать программы на языках общего назначения, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ;</p>	<p>ОПК-7.1 Знает современные языки программирования общего назначения; основы структурного и модульного программирования; современные технологии и методы программирования</p> <p>ОПК-7.2 Умеет формализовать поставленную задачу; применять соответствующий язык программирования при решении конкретных научных и практических задач; выбирать технологию и метод программирования для решения конкретной задачи</p> <p>ОПК-7.3 Владеет средствами разработки приложений для ОС реального режима работы микропроцессора; владеет средствами разработки приложений для ОС защищенного режима работы микропроцессора; владеет методами разработки приложений для решения профессиональных задач; навыками использования типовых ин-</p>	Алгоритмизация и программирование		
			Технологии и методы программирования		
			Б1.О.ДВ.02.01 Разработка моделей информационной безопасности		
			Б1.О.ДВ.02.02 Разработка моделей угроз безопасности автоматизированных систем		

<i>Категория (группа) ОПК (при наличии)</i>	<i>Код и наименование ОПК</i>	<i>Код и наименование индикатора достижения ОПК</i>	<i>Дисциплины / практики, участвующие в формировании ОПК</i>	<i>Практическая подготовка</i>	<i>Трудовая функция</i>
		струментальных средств программирования для решения профессиональных задач			
	ОПК-7.1. Способен использовать программные и программно-аппаратные средства для моделирования и испытания систем защиты информационных систем;	ОПК-7.1..1 Знает программные и программно-аппаратные средства для моделирования и испытания систем защиты информационных систем; методы применения программных и программно-аппаратных средств для моделирования и испытания систем защиты информационных систем ОПК-7.1..2 Умеет выбирать программные и программно-аппаратные средства для моделирования и испытания систем защиты информационных систем ОПК-7.1..3 Владеет навыками применения программных и программно-аппаратных средств для моделирования и испытания систем защиты информационных систем	Программно-аппаратные средства защиты информации		
	ОПК-7.2. Способен разрабатывать методики и тесты для анализа степени защищенности информационной системы и ее соответствия нормативным	ОПК-7.2..1 Знает основные подходы к проведению анализа защищенности автоматизированных систем, знает существующие методики и тесты для анализа степени защищенности информационной системы и её соответствия нормативным требованиям по защите информации	Инструментальная оценка эффективности систем защиты информации Оценка рисков информационной безопасности автоматизированных систем		

<i>Категория (группа) ОПК (при наличии)</i>	<i>Код и наименование ОПК</i>	<i>Код и наименование индикатора достижения ОПК</i>	<i>Дисциплины / практики, участвующие в формировании ОПК</i>	<i>Практическая подготовка</i>	<i>Трудовая функция</i>
	требованиям по защите информации;	ОПК-7.2..2 Умеет строить план проведения анализа системы защиты автоматизированных систем; умеет разрабатывать методики и тесты для анализа степени защищенности информационной системы и её соответствия нормативным требованиям по защите информации ОПК-7.2..3 Владеет навыком построения плана тестирования для проведения анализа защищенности; владеет методиками и навыками проведения тестов для анализа степени защищенности информационной системы и её соответствия нормативным требованиям по защите информации	Тестирование на проникновение и анализ безопасности		
	ОПК-7.3. Способен проводить анализ защищенности и верификацию программного обеспечения информационных систем;	ОПК-7.3..1 Знает виды и порядок проведения анализа защищенности автоматизированных систем ОПК-7.3..2 Умеет выбирать программное и аппаратное обеспечение для проведения анализа защищенности автоматизированных систем ОПК-7.3..3 Владеет навыками проведения анализа защищенности и верификации программного обеспечения автоматизированных систем	Анализ защищенности распределенных информационных систем		
Низкоуровневый анализ машинного кода					
Форензика					
	ОПК-8 Способен применять методы	ОПК-8.1 Знает основные перспективы развития науки и техники в области	Теория решения изобретательских за-		

<i>Категория (группа) ОПК (при наличии)</i>	<i>Код и наименование ОПК</i>	<i>Код и наименование индикатора достижения ОПК</i>	<i>Дисциплины / практики, участвующие в формировании ОПК</i>	<i>Практическая подготовка</i>	<i>Трудовая функция</i>
	научных исследований при проведении разработок в области защиты информации в автоматизированных системах;	защиты информации и автоматизированных систем, основные методы проведения научных исследований ОПК-8.2 Умеет применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами; умеет применять методы и системы искусственного интеллекта при реализации практических разработок в области защиты информации в автоматизированных системах ОПК-8.3 Владеет навыками применения научных методов в профессиональной деятельности; навыки решения научно-технических задач в области своей профессиональной деятельности	дач		
Системы интеллектуальной защиты информации					
Производственная практика (научно-исследовательская работа)					
	ОПК-9 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем	ОПК-9.1 Знает текущее состояние и тенденции развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации; порядок организации работ по технической защите конфиденциальной информации на объектах информатизации ОПК-9.2 Умеет планировать, организовывать и контролировать выполнение мероприятий по технической за-	Организация ЭВМ и вычислительных систем		
			Техническая защита информации		
			Сети и системы передачи информации		

<i>Категория (группа) ОПК (при наличии)</i>	<i>Код и наименование ОПК</i>	<i>Код и наименование индикатора достижения ОПК</i>	<i>Дисциплины / практики, участвующие в формировании ОПК</i>	<i>Практическая подготовка</i>	<i>Трудовая функция</i>
	передачи информации;	щите информации ОПК-9.3 Владеет методами проектирования и навыками эксплуатации систем и сетей передачи информации при решении задач профессиональной деятельности; навыками применения современных аппаратных устройств защиты информации и систем передачи информации			
	ОПК-10 Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности;	ОПК-10.1 Знает основы симметричной криптографии и криптографии с открытым ключом, основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах ОПК-10.2 Умеет использовать инфраструктуру открытых ключей, разрабатывать и анализировать программные модели средств криптографической защиты информации ОПК-10.3 Владеет навыками и подходами к анализу безопасности криптографических протоколов	Методы и средства криптографической защиты информации Безопасность сетей ЭВМ		
	ОПК-11 Способен разрабатывать компоненты систем защиты информации автоматизированных	ОПК-11.1 Знает программно-аппаратные средства, используемые в качестве компонентов систем защиты информации в программном обеспечении автоматизированных систем;	Разработка и эксплуатация автоматизированных систем в защищенном исполнении		

<i>Категория (группа) ОПК (при наличии)</i>	<i>Код и наименование ОПК</i>	<i>Код и наименование индикатора достижения ОПК</i>	<i>Дисциплины / практики, участвующие в формировании ОПК</i>	<i>Практическая подготовка</i>	<i>Трудовая функция</i>
	систем;	методы проектирования решений по обеспечению безопасности автоматизированных систем ОПК-11.2 Умеет проектировать защищенные распределенные информационные системы и компоненты систем защиты информации автоматизированных систем ОПК-11.3 Владеет навыками разработки компонентов систем защиты информации автоматизированных систем и защищенных распределенные информационные системы	Защита от хакерских угроз Программно-аппаратные средства защиты информации		
	ОПК-12 Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем;	ОПК-12.1 Знает принципы построения и функционирования, примеры реализации современных локальных и глобальных компьютерных сетей, операционных систем и баз данных; основы обеспечения информационной безопасности вычислительных сетей, операционных систем и баз данных ОПК-12.2 Умеет проектировать и администрировать компьютерные сети, реализовывать политику безопасности в сетях ЭВМ, операционных системах и базах данных ОПК-12.3 Владеет навыками построения и администрирования компьютерных сетей, администрирования операционных систем и баз данных с	Безопасность операционных систем Безопасность систем баз данных Администрирование распределенных информационных систем Безопасность сетей ЭВМ Администрирование систем и компьютерных сетей		

<i>Категория (группа) ОПК (при наличии)</i>	<i>Код и наименование ОПК</i>	<i>Код и наименование индикатора достижения ОПК</i>	<i>Дисциплины / практики, участвующие в формировании ОПК</i>	<i>Практическая подготовка</i>	<i>Трудовая функция</i>
		учетом требований по обеспечению безопасности			
	ОПК-13 Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем;	ОПК-13.1 Знает основные подходы к проведению анализа защищенности и тестирования систем защиты информации автоматизированных систем ОПК-13.2 Умеет выбирать программное и аппаратное обеспечение для проведения анализа защищенности и тестирования систем защиты информации; проводить анализ уязвимостей систем защиты информации автоматизированных систем ОПК-13.3 Владеет навыками проведения анализа защищенности автоматизированных систем, тестирования систем защиты информации автоматизированных систем, проведения анализа уязвимостей систем защиты информации автоматизированных систем	Анализ и защита веб-приложений		
			Анализ и защита мобильных приложений		
			Анализ защищенности распределенных информационных систем		
			Тестирование на проникновение и анализ безопасности		
	ОПК-14 Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, прово-	ОПК-14.1 Знает автоматизированные системы контроля информационной безопасности, систем защищенности и обеспечения их информационной безопасности ОПК-14.2 Умеет проводить подготовку исходных данных для технико-экономического обоснования проек-	Разработка и эксплуатация автоматизированных систем в защищенном исполнении		
			Б1.О.ДВ.01.01 Информационная безопасность предприя-		

<i>Категория (группа) ОПК (при наличии)</i>	<i>Код и наименование ОПК</i>	<i>Код и наименование индикатора достижения ОПК</i>	<i>Дисциплины / практики, участвующие в формировании ОПК</i>	<i>Практическая подготовка</i>	<i>Трудовая функция</i>
	дить подготовку исходных данных для технико-экономического обоснования проектных решений;	ных решений ОПК-14.3 Владеет навыком разработки защищенных автоматизированных систем, их эксплуатации и внедрения с учетом требований по защите информации	тия Б1.О.ДВ.01.02 Защита информации в информационных системах		
	ОПК-15 Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем;	ОПК-15.1 Знает средства и системы защиты информации автоматизированных систем, основные принципы администрирования защищенных компьютерных систем ОПК-15.2 Умеет выполнять функции администратора безопасности защищенных компьютерных систем ОПК-15.3 Владеет средствами администрирования программно-аппаратных комплексов защиты информации от несанкционированного доступа	Управление информационной безопасностью Тактическая защита периметра предприятия Стратегическая защита периметра предприятия		
	ОПК-16 Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования граждан-	ОПК-16.1 Знает основные тенденции в развитии российского государства, значимые факты и события из истории России в рассматриваемые периоды ОПК-16.2 Умеет анализировать и оценивать историческую информацию, факторы и механизмы исторических изменений ОПК-16.3 Владеет понятийно-			

<i>Категория (группа) ОПК (при наличии)</i>	<i>Код и наименование ОПК</i>	<i>Код и наименование индикатора достижения ОПК</i>	<i>Дисциплины / практики, участвующие в формировании ОПК</i>	<i>Практическая подготовка</i>	<i>Трудовая функция</i>
	ской позиции и развития патриотизма.	терминологическим аппаратом в области истории			

ПРОФЕССИОНАЛЬНЫЕ КОМПЕТЕНЦИИ (ПК)

<i>Основание</i>	<i>Код и наименование ПК</i>	<i>Код и наименование индикатора достижения ПК</i>	<i>Дисциплины / практики, участвующие в формировании ПК</i>	<i>Практическая подготовка</i>	<i>Трудовая функция</i>
- 06.033 «СПЕЦИАЛИСТ ПО ЗАЩИТЕ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ». Обобщенная трудовая функция: Д. Формирование требований к защите информации в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости	ПК-1 Способен проводить анализ структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем	ПК-1.1 Знает структурные и функциональные схемы защищенных автоматизированных систем ПК-1.2 Умеет проводить анализ структурных и функциональных схем защищенных автоматизированных информационных систем ПК-1.3 Владеет навыками выявления потенциальных уязвимостей информационной безопасности автоматизированных систем	Информационная безопасность объектов критической информационной инфраструктуры	- Частично	- ПС 06.033 ТФ 3.4.3 ТД-1 Проведение оценки показателей качества и эффективности работы вычислительных систем, программных и программно-аппаратных средств, используемых для построения систем защиты информации в автоматизированных системах - ПС 06.033 ТФ 3.4.3 ТД-2 Проведение технико-экономической оценки целесообразности создания системы защиты информации автоматизированной системы

<i>Основание</i>	<i>Код и наименование ПК</i>	<i>Код и наименование индикатора достижения ПК</i>	<i>Дисциплины / практики, участвующие в формировании ПК</i>	<i>Практическая подготовка</i>	<i>Трудовая функция</i>
					<ul style="list-style-type: none"> - ПС 06.033 ТФ 3.4.3 ТД-3 Определение порядка обработки информации в автоматизированной системе - ПС 06.033 ТФ 3.4.3 ТД-4 Формирование разделов технических заданий на создание систем защиты информации автоматизированных систем - ПС 06.033 ТФ 3.4.3 ТД-5 Разработка проектной документации на системы защиты автоматизированных систем - ПС 06.033 ТФ 3.4.3 ТД-6 Оформление заявки на разработку системы защиты информации автоматизированной системы
			Оценка рисков информационной безопасности автоматизированных систем	- Частично	<ul style="list-style-type: none"> - ПС 06.033 ТФ 3.4.3 НУ-1 Определять комплекс мер для обеспечения безопасности информационной в автоматизированных си-

<i>Основание</i>	<i>Код и наименование ПК</i>	<i>Код и наименование индикатора достижения ПК</i>	<i>Дисциплины / практики, участвующие в формировании ПК</i>	<i>Практическая подготовка</i>	<i>Трудовая функция</i>
					<p>стемах</p> <ul style="list-style-type: none"> - ПС 06.033 ТФ 3.4.3 НУ-2 Выявлять уязвимости информационных технологических ресурсов автоматизированных систем - ПС 06.033 ТФ 3.4.3 НУ-3 Разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем - ПС 06.033 ТФ 3.4.3 НУ-4 Проводить выбор программно-аппаратных средств обеспечения безопасности информации для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы - ПС 06.033 ТФ 3.4.3 НУ-5 Классифицировать и оценивать угрозы безопасности ин-

<i>Основание</i>	<i>Код и наименование ПК</i>	<i>Код и наименование индикатора достижения ПК</i>	<i>Дисциплины / практики, участвующие в формировании ПК</i>	<i>Практическая подготовка</i>	<i>Трудовая функция</i>
					<p>формации для автоматизированной системы - ПС 06.033 ТФ 3.4.3 НУ-6 Определять информационную инфраструктуру и информационные ресурсы автоматизированной системы, подлежащие защите - ПС 06.033 ТФ 3.4.3 НУ-7 Разрабатывать модели угроз безопасности информации и нарушителей в автоматизированных системах - ПС 06.033 ТФ 3.4.3 НУ-8 Определять эффективность применения средств информатизации</p>
			Производственная практика (преддипломная практика)	- Частично	- ПС 06.033 ТФ 3.4.1 ТД-1 Анализ характера обрабатываемой информации и определение перечня информации, подлежащей защите - ПС 06.033 ТФ 3.4.1 ТД-3 Планирование

<i>Основание</i>	<i>Код и наименование ПК</i>	<i>Код и наименование индикатора достижения ПК</i>	<i>Дисциплины / практики, участвующие в формировании ПК</i>	<i>Практическая подготовка</i>	<i>Трудовая функция</i>
					<p>мероприятий по обеспечению защиты информации в автоматизированной системе</p> <ul style="list-style-type: none"> - ПС 06.033 ТФ 3.4.1 ТД-4 Определение требуемого класса (уровня) защищенности автоматизированной системы - ПС 06.033 ТФ 3.4.1 НУ-1 Анализировать цели создания автоматизированных систем и задачи, решаемые автоматизированными системами - ПС 06.033 ТФ 3.4.1 НУ-4 Организовывать работы по созданию, внедрению, проектированию, разработке и сопровождению защищенных автоматизированных систем - ПС 06.033 ТФ 3.4.1 НЗ-5 Программно-аппаратные средства обеспечения защиты информации в программном обеспечении

<i>Основание</i>	<i>Код и наименование ПК</i>	<i>Код и наименование индикатора достижения ПК</i>	<i>Дисциплины / практики, участвующие в формировании ПК</i>	<i>Практическая подготовка</i>	<i>Трудовая функция</i>
					автоматизированных систем
<p>- 06.033 «СПЕЦИАЛИСТ ПО ЗАЩИТЕ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ».</p> <p>Обобщенная трудовая функция: D. Формирование требований к защите информации в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости</p>	<p>ПК-2 Способен проводить анализ защищенности информационной инфраструктуры автоматизированной системы</p>	<p>ПК-2.1 Знает способы проведения анализа защищенности информационной инфраструктуры автоматизированных систем</p> <p>ПК-2.2 Умеет выбирать способ проведения анализа защищенности информационной инфраструктуры автоматизированных систем</p> <p>ПК-2.3 Владеет навыками проведения анализа защищенности информационной инфраструктуры автоматизированных систем</p>	<p>Техника и технология атак злоумышленников в распределенных информационных системах</p>	<p>- Частично</p>	<p>- ПС 06.033 ТФ 3.4.3 НЗ-1 Основные информационные технологии, используемые в автоматизированных системах</p> <p>- ПС 06.033 ТФ 3.4.3 НЗ-2 Способы и средства защиты информации от несанкционированного доступа и утечки по техническим каналам и контроля эффективности защиты информации</p> <p>- ПС 06.033 ТФ 3.4.3 НЗ-3 Основные средства и способы обеспечения безопасности информации, принципы построения систем защиты информации</p> <p>- ПС 06.033 ТФ 3.4.3 НЗ-4 Программно-аппаратные средства обеспечения защиты информации автоматизированных систем</p>

<i>Основание</i>	<i>Код и наименование ПК</i>	<i>Код и наименование индикатора достижения ПК</i>	<i>Дисциплины / практики, участвующие в формировании ПК</i>	<i>Практическая подготовка</i>	<i>Трудовая функция</i>
					<ul style="list-style-type: none"> - ПС 06.033 ТФ 3.4.3 НЗ-5 Принципы построения средств защиты информации от несанкционированного доступа и утечки по техническим каналам - ПС 06.033 ТФ 3.4.3 НЗ-6 Национальные, межгосударственные и международные стандарты в области защиты информации - ПС 06.033 ТФ 3.4.3 НЗ-7 Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации - ПС 06.033 ТФ 3.4.3 НЗ-8 Организационные меры по защите информации - ПС 06.033 ТФ 3.4.3 НЗ-9 Методы тестирования и отладки, принципы организации документирования разработки, процесса сопровождения программно-

<i>Основание</i>	<i>Код и наименование ПК</i>	<i>Код и наименование индикатора достижения ПК</i>	<i>Дисциплины / практики, участвующие в формировании ПК</i>	<i>Практическая подготовка</i>	<i>Трудовая функция</i>
			Оценка рисков информационной безопасности автоматизированных систем	- Частично	<p>го обеспечения</p> <ul style="list-style-type: none"> - ПС 06.033 ТФ 3.4.2 НЗ-1 Основные информационные технологии, используемые в автоматизированных системах - ПС 06.033 ТФ 3.4.2 НЗ-2 Основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в вычислительных сетях - ПС 06.033 ТФ 3.4.2 НЗ-3 Программно-аппаратные средства обеспечения защиты информации автоматизированных систем - ПС 06.033 ТФ 3.4.2 НЗ-4 Способы реализации угроз безопасности в автоматизированных системах - ПС 06.033 ТФ 3.4.2 НЗ-5 Последствия от нарушения свойств безопасности информа-

<i>Основание</i>	<i>Код и наименование ПК</i>	<i>Код и наименование индикатора достижения ПК</i>	<i>Дисциплины / практики, участвующие в формировании ПК</i>	<i>Практическая подготовка</i>	<i>Трудовая функция</i>
					<p>ции</p> <ul style="list-style-type: none"> - ПС 06.033 ТФ 3.4.2 НЗ-6 Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах - ПС 06.033 ТФ 3.4.2 НЗ-7 Национальные, межгосударственные и международные стандарты в области защиты информации - ПС 06.033 ТФ 3.4.2 НЗ-8 Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации - ПС 06.033 ТФ 3.4.2 НЗ-9 Методики сертификационных испытаний технических средств защиты информации от несанкционированного доступа и утечки по техническим каналам на соответствие требованиям по безопасности ин-

<i>Основание</i>	<i>Код и наименование ПК</i>	<i>Код и наименование индикатора достижения ПК</i>	<i>Дисциплины / практики, участвующие в формировании ПК</i>	<i>Практическая подготовка</i>	<i>Трудовая функция</i>
					формации - ПС 06.033 ТФ 3.4.2 НЗ-10 Методы защиты информации от несанкционированного доступа и утечки по техническим каналам - ПС 06.033 ТФ 3.4.2 НЗ-11 Принципы формирования и реализации политики безопасности информации в автоматизированных системах
			Производственная практика (преддипломная практика)	- Частично	- ПС 06.033 ТФ 3.4.2 НУ-5 Выявлять известные уязвимости информационных систем - ПС 06.033 ТФ 3.4.2 НЗ-3 Программно-аппаратные средства обеспечения защиты информации автоматизированных систем - ПС 06.033 ТФ 3.4.2 НЗ-7 Национальные, межгосударственные и международные стандарты в области защиты информации

<i>Основание</i>	<i>Код и наименование ПК</i>	<i>Код и наименование индикатора достижения ПК</i>	<i>Дисциплины / практики, участвующие в формировании ПК</i>	<i>Практическая подготовка</i>	<i>Трудовая функция</i>
<p>- 06.033 «СПЕЦИАЛИСТ ПО ЗАЩИТЕ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ».</p> <p>Обобщенная трудовая функция: D. Формирование требований к защите информации в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости</p>	<p>ПК-3 Способен проводить анализ технической документации информационной инфраструктуры автоматизированной системы</p>	<p>ПК-3.1 Знает методики проведения анализа технической документации информационной инфраструктуры автоматизированной системы</p> <p>ПК-3.2 Умеет выбрать методику проведения анализа технической документации информационной инфраструктуры автоматизированной системы</p> <p>ПК-3.3 Владеет навыками проведения анализа технической документации информационной инфраструктуры автоматизированной системы</p>	<p>Информационная безопасность объектов критической информационной инфраструктуры</p>	<p>- Частично</p>	<p>- ПС 06.033 ТФ 3.4.1 НЗ-5 Программно-аппаратные средства обеспечения защиты информации в программном обеспечении автоматизированных систем</p> <p>- ПС 06.033 ТФ 3.4.1 НЗ-6 Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем</p> <p>- ПС 06.033 ТФ 3.4.1 НЗ-7 Принципы формирования политики информационной безопасности в автоматизированных системах</p> <p>- ПС 06.033 ТФ 3.4.1 НЗ-8 Нормативные правовые акты в области защиты информации</p> <p>- ПС 06.033 ТФ 3.4.1 НЗ-9 Национальные, межгосударственные и международные стандарты в области защи-</p>

<i>Основание</i>	<i>Код и наименование ПК</i>	<i>Код и наименование индикатора достижения ПК</i>	<i>Дисциплины / практики, участвующие в формировании ПК</i>	<i>Практическая подготовка</i>	<i>Трудовая функция</i>
					<p>ты информации</p> <ul style="list-style-type: none"> - ПС 06.033 ТФ 3.4.1 НЗ-10 Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации - ПС 06.033 ТФ 3.4.1 НЗ-11 Организационные меры по защите информации - ПС 06.033 ТФ 3.4.1 НЗ-12 Методики сертификационных испытаний технических средств защиты информации от несанкционированного доступа и утечки по техническим каналам на соответствие требованиям по безопасности информации - ПС 06.033 ТФ 3.4.1 НЗ-13 Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты

<i>Основание</i>	<i>Код и наименование ПК</i>	<i>Код и наименование индикатора достижения ПК</i>	<i>Дисциплины / практики, участвующие в формировании ПК</i>	<i>Практическая подготовка</i>	<i>Трудовая функция</i>
			Аттестация объектов информатизации	- Частично	<p>информации</p> <ul style="list-style-type: none"> - ПС 06.033 ТФ 3.4.1 НУ-1 Анализировать цели создания автоматизированных систем и задачи, решаемые автоматизированными системами - ПС 06.033 ТФ 3.4.1 НУ-2 Выявлять уязвимости информационно-технологических ресурсов автоматизированных систем - ПС 06.033 ТФ 3.4.1 НУ-3 Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности и оценивать угрозы безопасности информации - ПС 06.033 ТФ 3.4.1 НУ-4 Организовывать работы по созданию, внедрению, проектированию, разработке и сопровождению защищенных автоматизированных систем

<i>Основание</i>	<i>Код и наименование ПК</i>	<i>Код и наименование индикатора достижения ПК</i>	<i>Дисциплины / практики, участвующие в формировании ПК</i>	<i>Практическая подготовка</i>	<i>Трудовая функция</i>
					<ul style="list-style-type: none"> - ПС 06.033 ТФ 3.4.1 НУ-5 Использовать рисковую методологию управления защитой информации в автоматизированной системе - ПС 06.033 ТФ 3.4.1 НУ-6 Определять класс защищенности автоматизированных систем и ее составных частей
			Производственная практика (преддипломная практика)	- Частично	<ul style="list-style-type: none"> - ПС 06.033 ТФ 3.4.2 НЗ-10 Методы защиты информации от несанкционированного доступа и утечки по техническим каналам - ПС 06.033 ТФ 3.4.3 ТД-3 Определение порядка обработки информации в автоматизированной системе - ПС 06.033 ТФ 3.4.3 НУ-3 Разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем

<i>Основание</i>	<i>Код и наименование ПК</i>	<i>Код и наименование индикатора достижения ПК</i>	<i>Дисциплины / практики, участвующие в формировании ПК</i>	<i>Практическая подготовка</i>	<i>Трудовая функция</i>
<p>- 06.033 «СПЕЦИАЛИСТ ПО ЗАЩИТЕ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ».</p> <p>Обобщенная трудовая функция: D. Формирование требований к защите информации в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости</p>	<p>ПК-4 Способен анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах</p>	<p>ПК-4.1 Знает программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем</p> <p>ПК-4.2 Умеет выбрать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах</p> <p>ПК-4.3 Владеет навыками анализа программных, архитектурно-технических и схемотехнических решений компонентов автоматизированных систем с целью выявления потенци-</p>	<p>Аппараты и средства перехвата информации</p>	<p>- Частично</p>	<p>- ПС 06.033 ТФ 3.4.2 ТД-1 Формирование разделов технических заданий на создание систем защиты информации автоматизированных систем</p> <p>- ПС 06.033 ТФ 3.4.2 ТД-2 Разработка систем защиты информации автоматизированных систем с учетом действующих нормативно-правовых документов</p> <p>- ПС 06.033 ТФ 3.4.2 ТД-3 Определение комплекса мер (правил, процедур, практических приемов, руководящих принципов, методов, средств) для защиты информации автоматизированных систем</p> <p>- ПС 06.033 ТФ 3.4.2 ТД-4 Определение оценки возможностей внешних и внутренних нарушителей</p> <p>- ПС 06.033 ТФ 3.4.2 ТД-5 Разработка моде-</p>

<i>Основание</i>	<i>Код и наименование ПК</i>	<i>Код и наименование индикатора достижения ПК</i>	<i>Дисциплины / практики, участвующие в формировании ПК</i>	<i>Практическая подготовка</i>	<i>Трудовая функция</i>
		<p>альных уязвимостей безопасности информации в автоматизированных системах</p>			<p>ли угроз безопасности информации автоматизированной системы - ПС 06.033 ТФ 3.4.2 ТД-6 Обоснование перечня сертифицированных средств защиты информации, необходимых для создания системы защиты информации автоматизированной системы - ПС 06.033 ТФ 3.4.2 ТД-7 Анализ требований к назначению, структуре и конфигурации создаваемой автоматизированной системы с целью выявления угроз безопасности информации - ПС 06.033 ТФ 3.4.2 ТД-8 Определение структурно-функциональных характеристик информационной системы в соответствии с требованиями нормативных правовых документов в области защиты ин-</p>

<i>Основание</i>	<i>Код и наименование ПК</i>	<i>Код и наименование индикатора достижения ПК</i>	<i>Дисциплины / практики, участвующие в формировании ПК</i>	<i>Практическая подготовка</i>	<i>Трудовая функция</i>
					формации в автоматизированных системах
			Защищенные автоматизированные системы	- Частично	<p>- ПС 06.033 ТФ 3.4.2 НУ-1 Производить выбор программно-аппаратных средств защиты информации для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности информации в автоматизированной системе</p> <p>- ПС 06.033 ТФ 3.4.2 НУ-2 Формировать перечень мероприятий по предотвращению угроз безопасности информации автоматизированной системы</p> <p>- ПС 06.033 ТФ 3.4.2 НУ-3 Систематизировать результаты проведенных исследований</p> <p>- ПС 06.033 ТФ 3.4.2 НУ-4 Анализировать возможные уязвимости информационных си-</p>

<i>Основание</i>	<i>Код и наименование ПК</i>	<i>Код и наименование индикатора достижения ПК</i>	<i>Дисциплины / практики, участвующие в формировании ПК</i>	<i>Практическая подготовка</i>	<i>Трудовая функция</i>
					<p>стем</p> <ul style="list-style-type: none"> - ПС 06.033 ТФ 3.4.2 НУ-5 Выявлять известные уязвимости информационных систем - ПС 06.033 ТФ 3.4.2 НУ-6 Разрабатывать проекты нормативных документов, регламентирующих работу по защите информации в автоматизированных системах
			<p>Производственная практика (преддипломная практика)</p>	<p>- Частично</p>	<ul style="list-style-type: none"> - ПС 06.033 ТФ 3.4.3 НУ-5 Классифицировать и оценивать угрозы безопасности информации для автоматизированной системы - ПС 06.033 ТФ 3.4.3 НУ-8 Определять эффективность применения средств информатизации - ПС 06.033 ТФ 3.4.3 НЗ-6 Национальные, межгосударственные и международные стандарты в области защиты информации

<i>Основание</i>	<i>Код и наименование ПК</i>	<i>Код и наименование индикатора достижения ПК</i>	<i>Дисциплины / практики, участвующие в формировании ПК</i>	<i>Практическая подготовка</i>	<i>Трудовая функция</i>
<p>- 06.033 «СПЕЦИАЛИСТ ПО ЗАЩИТЕ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ».</p> <p>Обобщенная трудовая функция: Д. Формирование требований к защите информации в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости</p>	<p>ПК-5 Способен контролировать безотказное функционирование технических средств защиты информации</p>	<p>ПК-5.1 Знает способы контроля безотказного функционирования технических средств защиты информации</p> <p>ПК-5.2 Умеет выбрать способ контроля безотказного функционирования технических средств защиты информации</p> <p>ПК-5.3 Владеет навыками контроля безотказного функционирования технических средств защиты информации</p>	<p>Б1.В.ДВ.03.01 Защита информации в автоматизированных системах кредитно-финансовой сферы</p>	<p>- Частично</p>	<p>- ПС 06.033 ТФ 3.4.4 НЗ-1 Методы и технологии проектирования, моделирования, исследования систем защиты информации автоматизированных систем</p> <p>- ПС 06.033 ТФ 3.4.4 НЗ-2 Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах</p> <p>- ПС 06.033 ТФ 3.4.4 НЗ-3 Основные меры по защите информации в автоматизированных системах</p> <p>- ПС 06.033 ТФ 3.4.4 НЗ-4 Национальные, межгосударственные и международные стандарты в области защиты информации</p> <p>- ПС 06.033 ТФ 3.4.4 НЗ-5 Руководящие и методические документы уполномоченных федеральных органов исполнительной власти</p>

<i>Основание</i>	<i>Код и наименование ПК</i>	<i>Код и наименование индикатора достижения ПК</i>	<i>Дисциплины / практики, участвующие в формировании ПК</i>	<i>Практическая подготовка</i>	<i>Трудовая функция</i>
					<p>по защите информации</p> <ul style="list-style-type: none"> - ПС 06.033 ТФ 3.4.4 НЗ-6 Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах - ПС 06.033 ТФ 3.4.4 НЗ-7 Принципы построения средств защиты информации от несанкционированного доступа и утечки по техническим каналам - ПС 06.033 ТФ 3.4.4 НЗ-8 Принципы построения и функционирования систем и сетей передачи информации
			<p>Б1.В.ДВ.03.02 Обеспечение информационной безопасности в банковской сфере</p>	<p>- Частично</p>	<ul style="list-style-type: none"> - ПС 06.033 ТФ 3.4.4 НЗ-1 Методы и технологии проектирования, моделирования, исследования систем защиты информации автоматизированных систем - ПС 06.033 ТФ 3.4.4 НЗ-2 Основные угрозы

<i>Основание</i>	<i>Код и наименование ПК</i>	<i>Код и наименование индикатора достижения ПК</i>	<i>Дисциплины / практики, участвующие в формировании ПК</i>	<i>Практическая подготовка</i>	<i>Трудовая функция</i>
					<p>безопасности информации и модели нарушителя в автоматизированных системах - ПС 06.033 ТФ 3.4.4 НЗ-3 Основные меры по защите информации в автоматизированных системах - ПС 06.033 ТФ 3.4.4 НЗ-4 Национальные, межгосударственные и международные стандарты в области защиты информации - ПС 06.033 ТФ 3.4.4 НЗ-5 Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации - ПС 06.033 ТФ 3.4.4 НЗ-6 Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах - ПС 06.033 ТФ 3.4.4</p>

<i>Основание</i>	<i>Код и наименование ПК</i>	<i>Код и наименование индикатора достижения ПК</i>	<i>Дисциплины / практики, участвующие в формировании ПК</i>	<i>Практическая подготовка</i>	<i>Трудовая функция</i>
					<p>НЗ-7 Принципы построения средств защиты информации от несанкционированного доступа и утечки по техническим каналам - ПС 06.033 ТФ 3.4.4</p> <p>НЗ-8 Принципы построения и функционирования систем и сетей передачи информации</p>
			<p>Б1.В.ДВ.04.01 Защита информации при передаче по открытым каналам связи</p>	<p>- Частично</p>	<p>- ПС 06.033 ТФ 3.4.3</p> <p>НУ-1 Определять комплекс мер для обеспечения безопасности информационной в автоматизированных системах - ПС 06.033 ТФ 3.4.3</p> <p>НУ-2 Выявлять уязвимости информационно-технологических ресурсов автоматизированных систем - ПС 06.033 ТФ 3.4.3</p> <p>НУ-3 Разрабатывать предложения по совершенствованию системы управления защиты информации автоматизи-</p>

<i>Основание</i>	<i>Код и наименование ПК</i>	<i>Код и наименование индикатора достижения ПК</i>	<i>Дисциплины / практики, участвующие в формировании ПК</i>	<i>Практическая подготовка</i>	<i>Трудовая функция</i>
					<p>зированных систем - ПС 06.033 ТФ 3.4.3 НУ-4 Проводить выбор программно-аппаратных средств обеспечения безопасности информации для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы - ПС 06.033 ТФ 3.4.3 НУ-5 Классифицировать и оценивать угрозы безопасности информации для автоматизированной системы - ПС 06.033 ТФ 3.4.3 НУ-6 Определять информационную инфраструктуру и информационные ресурсы автоматизированной системы, подлежащие защите - ПС 06.033 ТФ 3.4.3 НУ-7 Разрабатывать модели угроз безопас-</p>

<i>Основание</i>	<i>Код и наименование ПК</i>	<i>Код и наименование индикатора достижения ПК</i>	<i>Дисциплины / практики, участвующие в формировании ПК</i>	<i>Практическая подготовка</i>	<i>Трудовая функция</i>
					ности информации и нарушителей в автоматизированных системах - ПС 06.033 ТФ 3.4.3 НУ-8 Определять эффективность применения средств информатизации
			Б1.В.ДВ.04.02 Обеспечение информационной безопасности в перинетовых сетях	- Частично	- ПС 06.033 ТФ 3.4.3 НУ-1 Определять комплекс мер для обеспечения безопасности информационной в автоматизированных системах - ПС 06.033 ТФ 3.4.3 НУ-2 Выявлять уязвимости информационно-технологических ресурсов автоматизированных систем - ПС 06.033 ТФ 3.4.3 НУ-3 Разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем - ПС 06.033 ТФ 3.4.3 НУ-4 Проводить выбор

<i>Основание</i>	<i>Код и наименование ПК</i>	<i>Код и наименование индикатора достижения ПК</i>	<i>Дисциплины / практики, участвующие в формировании ПК</i>	<i>Практическая подготовка</i>	<i>Трудовая функция</i>
					<p>программно-аппаратных средств обеспечения безопасности информации для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы</p> <p>- ПС 06.033 ТФ 3.4.3 НУ-5 Классифицировать и оценивать угрозы безопасности информации для автоматизированной системы</p> <p>- ПС 06.033 ТФ 3.4.3 НУ-6 Определять информационную инфраструктуру и информационные ресурсы автоматизированной системы, подлежащие защите</p> <p>- ПС 06.033 ТФ 3.4.3 НУ-7 Разрабатывать модели угроз безопасности информации и нарушителей в автоматизированных системах</p>

<i>Основание</i>	<i>Код и наименование ПК</i>	<i>Код и наименование индикатора достижения ПК</i>	<i>Дисциплины / практики, участвующие в формировании ПК</i>	<i>Практическая подготовка</i>	<i>Трудовая функция</i>
					- ПС 06.033 ТФ 3.4.3 НУ-8 Определять эффективность применения средств информатизации
			Производственная практика (технологическая практика)	- Частично	- ПС 06.033 ТФ 3.4.3 НЗ-6 Национальные, межгосударственные и международные стандарты в области защиты информации - ПС 06.033 ТФ 3.4.3 НЗ-7 Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации - ПС 06.033 ТФ 3.4.3 НЗ-8 Организационные меры по защите информации
- 06.033 «СПЕЦИАЛИСТ ПО ЗАЩИТЕ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ». Обобщенная трудовая функция: Д. Формирование требований к защите информа-	ПК-6 Способен проектировать подсистемы безопасности информации с учетом действующих нормативных и методических доку-	ПК-6.1 Знает способы проектирования подсистем безопасности информации с учетом действующих нормативных и методических доку-	Аттестация объектов информатизации	- Частично	- ПС 06.033 ТФ 3.4.1 ТД-1 Анализ характера обрабатываемой информации и определение перечня информации, подлежащей защите

<i>Основание</i>	<i>Код и наименование ПК</i>	<i>Код и наименование индикатора достижения ПК</i>	<i>Дисциплины / практики, участвующие в формировании ПК</i>	<i>Практическая подготовка</i>	<i>Трудовая функция</i>
<p>ции в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости</p>	<p>ментов</p>	<p>ментов ПК-6.2 Умеет выбрать способ проектирования подсистем безопасности информации с учетом действующих нормативных и методических документов ПК-6.3 Владеет навыками проектирования подсистем безопасности информации с учетом действующих нормативных и методических документов</p>			<p>- ПС 06.033 ТФ 3.4.1 ТД-2 Выявление степени участия персонала в обработке защищаемой информации - ПС 06.033 ТФ 3.4.1 ТД-3 Планирование мероприятий по обеспечению защиты информации в автоматизированной системе - ПС 06.033 ТФ 3.4.1 ТД-4 Определение требуемого класса (уровня) защищенности автоматизированной системы - ПС 06.033 ТФ 3.4.1 ТД-5 Обоснование необходимости использования криптографических средств защиты информации - ПС 06.033 ТФ 3.4.1 ТД-6 Разработка отчетных документов и разделов технических заданий</p>
			<p>Руководство и управление службой</p>	<p>- Частично</p>	<p>- ПС 06.033 ТФ 3.4.4 ТД-1 Разработка анали-</p>

<i>Основание</i>	<i>Код и наименование ПК</i>	<i>Код и наименование индикатора достижения ПК</i>	<i>Дисциплины / практики, участвующие в формировании ПК</i>	<i>Практическая подготовка</i>	<i>Трудовая функция</i>
			безопасности		<p>тических и компьютерных моделей автоматизированных систем и подсистем безопасности автоматизированных систем</p> <p>- ПС 06.033 ТФ 3.4.4 ТД-2 Исследование аналитических и компьютерных моделей автоматизированных систем и подсистем безопасности автоматизированных систем</p> <p>- ПС 06.033 ТФ 3.4.4 ТД-3 Разработка модели угроз безопасности информации и нарушителей в автоматизированных системах</p> <p>- ПС 06.033 ТФ 3.4.4 ТД-4 Исследование программных, архитектурно-технических и схемотехнических решений компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в</p>

<i>Основание</i>	<i>Код и наименование ПК</i>	<i>Код и наименование индикатора достижения ПК</i>	<i>Дисциплины / практики, участвующие в формировании ПК</i>	<i>Практическая подготовка</i>	<i>Трудовая функция</i>
					автоматизированных системах - ПС 06.033 ТФ 3.4.4 ТД-5 Анализ информационной инфраструктуры и безопасности информации автоматизированных систем - ПС 06.033 ТФ 3.4.4 ТД-6 Разработка предложений по совершенствованию системы управления информационной безопасностью автоматизированных систем
			Б1.В.ДВ.02.01 Информационная безопасность распределенных информационных систем	- Частично	- ПС 06.033 ТФ 3.4.4 НУ-1 Выполнять сбор, обработку, анализ и систематизацию научно-технической информации в области защиты информации - ПС 06.033 ТФ 3.4.4 НУ-2 Разрабатывать и исследовать математические модели конкретных явлений и процессов для решения расчетных и исследова-

<i>Основание</i>	<i>Код и наименование ПК</i>	<i>Код и наименование индикатора достижения ПК</i>	<i>Дисциплины / практики, участвующие в формировании ПК</i>	<i>Практическая подготовка</i>	<i>Трудовая функция</i>
					<p>тельских задач</p> <ul style="list-style-type: none"> - ПС 06.033 ТФ 3.4.4 НУ-3 Применять математические модели при проектировании систем защиты информации автоматизированных систем - ПС 06.033 ТФ 3.4.4 НУ-4 Проектировать и реализовывать политику безопасности вычислительных сетей - ПС 06.033 ТФ 3.4.4 НУ-5 Анализировать основные характеристики и возможности телекоммуникационных систем по передаче информации
			Б1.В.ДВ.02.02 Информационная безопасность систем распределенной обработки информации	- Частично	<ul style="list-style-type: none"> - ПС 06.033 ТФ 3.4.4 НУ-1 Выполнять сбор, обработку, анализ и систематизацию научно-технической информации в области защиты информации - ПС 06.033 ТФ 3.4.4 НУ-2 Разрабатывать и исследовать математи-

<i>Основание</i>	<i>Код и наименование ПК</i>	<i>Код и наименование индикатора достижения ПК</i>	<i>Дисциплины / практики, участвующие в формировании ПК</i>	<i>Практическая подготовка</i>	<i>Трудовая функция</i>
					<p>ческие модели конкретных явлений и процессов для решения расчетных и исследовательских задач</p> <p>- ПС 06.033 ТФ 3.4.4 НУ-3 Применять математические модели при проектировании систем защиты информации автоматизированных систем</p> <p>- ПС 06.033 ТФ 3.4.4 НУ-4 Проектировать и реализовывать политику безопасности вычислительных сетей</p> <p>- ПС 06.033 ТФ 3.4.4 НУ-5 Анализировать основные характеристики и возможности телекоммуникационных систем по передаче информации</p>
			Б1.О.ДВ.01.01 Информационная безопасность предприятия	- Частично	- ПС 06.033 ТФ 3.4.4 НЗ-1 Методы и технологии проектирования, моделирования, исследования систем защиты информации автоматизи-

<i>Основание</i>	<i>Код и наименование ПК</i>	<i>Код и наименование индикатора достижения ПК</i>	<i>Дисциплины / практики, участвующие в формировании ПК</i>	<i>Практическая подготовка</i>	<i>Трудовая функция</i>
					<p>зированных систем</p> <ul style="list-style-type: none"> - ПС 06.033 ТФ 3.4.4 НЗ-2 Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах - ПС 06.033 ТФ 3.4.4 НЗ-3 Основные меры по защите информации в автоматизированных системах - ПС 06.033 ТФ 3.4.4 НЗ-4 Национальные, межгосударственные и международные стандарты в области защиты информации - ПС 06.033 ТФ 3.4.4 НЗ-5 Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации - ПС 06.033 ТФ 3.4.4 НЗ-6 Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в

<i>Основание</i>	<i>Код и наименование ПК</i>	<i>Код и наименование индикатора достижения ПК</i>	<i>Дисциплины / практики, участвующие в формировании ПК</i>	<i>Практическая подготовка</i>	<i>Трудовая функция</i>
					автоматизированных системах - ПС 06.033 ТФ 3.4.4 НЗ-7 Принципы построения средств защиты информации от несанкционированного доступа и утечки по техническим каналам - ПС 06.033 ТФ 3.4.4 НЗ-8 Принципы построения и функционирования систем и сетей передачи информации
			Б1.О.ДВ.01.02 Защита информации в информационных системах	- Частично	- ПС 06.033 ТФ 3.4.4 НЗ-1 Методы и технологии проектирования, моделирования, исследования систем защиты информации автоматизированных систем - ПС 06.033 ТФ 3.4.4 НЗ-2 Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах - ПС 06.033 ТФ 3.4.4 НЗ-3 Основные меры по защите информации

<i>Основание</i>	<i>Код и наименование ПК</i>	<i>Код и наименование индикатора достижения ПК</i>	<i>Дисциплины / практики, участвующие в формировании ПК</i>	<i>Практическая подготовка</i>	<i>Трудовая функция</i>
					<p>в автоматизированных системах</p> <ul style="list-style-type: none"> - ПС 06.033 ТФ 3.4.4 НЗ-4 Национальные, межгосударственные и международные стандарты в области защиты информации - ПС 06.033 ТФ 3.4.4 НЗ-5 Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации - ПС 06.033 ТФ 3.4.4 НЗ-6 Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах - ПС 06.033 ТФ 3.4.4 НЗ-7 Принципы построения средств защиты информации от несанкционированного доступа и утечки по техническим каналам <p>- ПС 06.033 ТФ 3.4.4</p>

<i>Основание</i>	<i>Код и наименование ПК</i>	<i>Код и наименование индикатора достижения ПК</i>	<i>Дисциплины / практики, участвующие в формировании ПК</i>	<i>Практическая подготовка</i>	<i>Трудовая функция</i>
					НЗ-8 Принципы построения и функционирования систем и сетей передачи информации
			Производственная практика (проектно-технологическая практика), 11 семестр	- Частично	- ПС 06.033 ТФ 3.4.3 НЗ-8 Организационные меры по защите информации - ПС 06.033 ТФ 3.4.4 ТД-2 Исследование аналитических и компьютерных моделей автоматизированных систем и подсистем безопасности автоматизированных систем - ПС 06.033 ТФ 3.4.4 ТД-5 Анализ информационной инфраструктуры и безопасности информации автоматизированных систем
			Производственная практика (преддипломная практика)	- Частично	- ПС 06.033 ТФ 3.4.4 ТД-5 Анализ информационной инфраструктуры и безопасности информации автоматизированных систем - ПС 06.033 ТФ 3.4.4

<i>Основание</i>	<i>Код и наименование ПК</i>	<i>Код и наименование индикатора достижения ПК</i>	<i>Дисциплины / практики, участвующие в формировании ПК</i>	<i>Практическая подготовка</i>	<i>Трудовая функция</i>
					НУ-1 Выполнять сбор, обработку, анализ и систематизацию научно-технической информации в области защиты информации - ПС 06.033 ТФ 3.4.4 НУ-4 Проектировать и реализовывать политику безопасности вычислительных сетей - ПС 06.033 ТФ 3.4.4 НЗ-3 Основные меры по защите информации в автоматизированных системах

Профессиональный стандарт 06.033 (ПС 06.033) «СПЕЦИАЛИСТ ПО ЗАЩИТЕ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ»

Обобщенная трудовая функция: D. Формирование требований к защите информации в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости

3.4.1 Трудовая функция (ТФ 3.4.1)

Наименование	Обоснование необходимости защиты информации в автоматизированной системе	Код	D/01.7	Уровень (подуровень) квалификации	7
--------------	--	-----	--------	-----------------------------------	---

Трудовые действия	ТД-1 Анализ характера обрабатываемой информации и определение перечня информации, подлежащей защите
	ТД-2 Выявление степени участия персонала в обработке защищаемой информации
	ТД-3 Планирование мероприятий по обеспечению защиты информации в автоматизированной системе
	ТД-4 Определение требуемого класса (уровня) защищенности автоматизированной системы
	ТД-5 Обоснование необходимости использования криптографических средств защиты информации
	ТД-6 Разработка отчетных документов и разделов технических заданий
Необходимые умения	НУ-1 Анализировать цели создания автоматизированных систем и задачи, решаемые автоматизированными системами
	НУ-2 Выявлять уязвимости информационно-технологических ресурсов автоматизированных систем
	НУ-3 Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности и оценивать угрозы безопасности информации
	НУ-4 Организовывать работы по созданию, внедрению, проектированию, разработке и сопровождению защищенных автоматизированных систем
	НУ-5 Использовать рисковую методологию управления защитой информации в автоматизированной системе
	НУ-6 Определять класс защищенности автоматизированных систем и ее составных частей
Необходимые знания	НЗ-1 Основные информационные технологии, используемые в автоматизированных системах
	НЗ-2 Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах
	НЗ-3 Виды информационных воздействий и критерии оценки защищенности информации в автоматизированных системах
	НЗ-4 Методы защиты информации от несанкционированного доступа и утечки по техническим каналам
	НЗ-5 Программно-аппаратные средства обеспечения защиты информации в программном обеспечении автоматизированных систем
	НЗ-6 Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем
	НЗ-7 Принципы формирования политики информационной безопасности в автоматизированных системах
	НЗ-8 Нормативные правовые акты в области защиты информации
	НЗ-9 Национальные, межгосударственные и международные стандарты в области защиты информации
	НЗ-10 Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации
	НЗ-11 Организационные меры по защите информации
	НЗ-12 Методики сертификационных испытаний технических средств защиты информации от несанкционированно-

	го доступа и утечки по техническим каналам на соответствие требованиям по безопасности информации
	НЗ-13 Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации

3.4.2 Трудовая функция (ТФ 3.4.2)

Наименование	Определение угроз безопасности информации, обрабатываемой автоматизированной системой	Код	D/02.7	Уровень (подуровень) квалификации	7
--------------	---	-----	--------	-----------------------------------	---

Трудовые действия	ТД-1 Формирование разделов технических заданий на создание систем защиты информации автоматизированных систем
	ТД-2 Разработка систем защиты информации автоматизированных систем с учетом действующих нормативно-правовых документов
	ТД-3 Определение комплекса мер (правил, процедур, практических приемов, руководящих принципов, методов, средств) для защиты информации автоматизированных систем
	ТД-4 Определение оценки возможностей внешних и внутренних нарушителей
	ТД-5 Разработка модели угроз безопасности информации автоматизированной системы
	ТД-6 Обоснование перечня сертифицированных средств защиты информации, необходимых для создания системы защиты информации автоматизированной системы
	ТД-7 Анализ требований к назначению, структуре и конфигурации создаваемой автоматизированной системы с целью выявления угроз безопасности информации
	ТД-8 Определение структурно-функциональных характеристик информационной системы в соответствии с требованиями нормативных правовых документов в области защиты информации в автоматизированных системах
Необходимые умения	НУ-1 Производить выбор программно-аппаратных средств защиты информации для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности информации в автоматизированной системе
	НУ-2 Формировать перечень мероприятий по предотвращению угроз безопасности информации автоматизированной системы
	НУ-3 Систематизировать результаты проведенных исследований
	НУ-4 Анализировать возможные уязвимости информационных систем
	НУ-5 Выявлять известные уязвимости информационных систем

	НУ-6 Разрабатывать проекты нормативных документов, регламентирующих работу по защите информации в автоматизированных системах
Необходимые знания	НЗ-1 Основные информационные технологии, используемые в автоматизированных системах
	НЗ-2 Основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в вычислительных сетях
	НЗ-3 Программно-аппаратные средства обеспечения защиты информации автоматизированных систем
	НЗ-4 Способы реализации угроз безопасности в автоматизированных системах
	НЗ-5 Последствия от нарушения свойств безопасности информации
	НЗ-6 Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах
	НЗ-7 Национальные, межгосударственные и международные стандарты в области защиты информации
	НЗ-8 Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации
	НЗ-9 Методики сертификационных испытаний технических средств защиты информации от несанкционированного доступа и утечки по техническим каналам на соответствие требованиям по безопасности информации
	НЗ-10 Методы защиты информации от несанкционированного доступа и утечки по техническим каналам
	НЗ-11 Принципы формирования и реализации политики безопасности информации в автоматизированных системах

3.4.3 Трудовая функция (ТФ 3.4.3)

Наименование	Разработка архитектуры системы защиты информации автоматизированной системы	Код	D/03.7	Уровень (подуровень) квалификации	7
--------------	---	-----	--------	-----------------------------------	---

Трудовые действия	ТД-1 Проведение оценки показателей качества и эффективности работы вычислительных систем, программных и программно-аппаратных средств, используемых для построения систем защиты информации в автоматизированных системах
	ТД-2 Проведение технико-экономической оценки целесообразности создания системы защиты информации автоматизированной системы
	ТД-3 Определение порядка обработки информации в автоматизированной системе
	ТД-4 Формирование разделов технических заданий на создание систем защиты информации автоматизированных систем

	ТД-5 Разработка проектной документации на системы защиты автоматизированных систем
	ТД-6 Оформление заявки на разработку системы защиты информации автоматизированной системы
Необходимые умения	НУ-1 Определять комплекс мер для обеспечения безопасности информационной в автоматизированных системах
	НУ-2 Выявлять уязвимости информационно-технологических ресурсов автоматизированных систем
	НУ-3 Разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем
	НУ-4 Проводить выбор программно-аппаратных средств обеспечения безопасности информации для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы
	НУ-5 Классифицировать и оценивать угрозы безопасности информации для автоматизированной системы
	НУ-6 Определять информационную инфраструктуру и информационные ресурсы автоматизированной системы, подлежащие защите
	НУ-7 Разрабатывать модели угроз безопасности информации и нарушителей в автоматизированных системах
	НУ-8 Определять эффективность применения средств информатизации
Необходимые знания	НЗ-1 Основные информационные технологии, используемые в автоматизированных системах
	НЗ-2 Способы и средства защиты информации от несанкционированного доступа и утечки по техническим каналам и контроля эффективности защиты информации
	НЗ-3 Основные средства и способы обеспечения безопасности информации, принципы построения систем защиты информации
	НЗ-4 Программно-аппаратные средства обеспечения защиты информации автоматизированных систем
	НЗ-5 Принципы построения средств защиты информации от несанкционированного доступа и утечки по техническим каналам
	НЗ-6 Национальные, межгосударственные и международные стандарты в области защиты информации
	НЗ-7 Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации
	НЗ-8 Организационные меры по защите информации
	НЗ-9 Методы тестирования и отладки, принципы организации документирования разработки, процесса сопровождения программного обеспечения

3.4.4 Трудовая функция (ТФ 3.4.4)

Наименование

Моделирование защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации

Код

D/04.7

Уровень (подуровень) квалификации

7

Трудовые действия	ТД-1 Разработка аналитических и компьютерных моделей автоматизированных систем и подсистем безопасности автоматизированных систем
	ТД-2 Исследование аналитических и компьютерных моделей автоматизированных систем и подсистем безопасности автоматизированных систем
	ТД-3 Разработка модели угроз безопасности информации и нарушителей в автоматизированных системах
	ТД-4 Исследование программных, архитектурно-технических и схемотехнических решений компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах
	ТД-5 Анализ информационной инфраструктуры и безопасности информации автоматизированных систем
	ТД-6 Разработка предложений по совершенствованию системы управления информационной безопасностью автоматизированных систем
Необходимые умения	НУ-1 Выполнять сбор, обработку, анализ и систематизацию научно-технической информации в области защиты информации
	НУ-2 Разрабатывать и исследовать математические модели конкретных явлений и процессов для решения расчетных и исследовательских задач
	НУ-3 Применять математические модели при проектировании систем защиты информации автоматизированных систем
	НУ-4 Проектировать и реализовывать политику безопасности вычислительных сетей
	НУ-5 Анализировать основные характеристики и возможности телекоммуникационных систем по передаче информации
Необходимые знания	НЗ-1 Методы и технологии проектирования, моделирования, исследования систем защиты информации автоматизированных систем
	НЗ-2 Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах
	НЗ-3 Основные меры по защите информации в автоматизированных системах
	НЗ-4 Национальные, межгосударственные и международные стандарты в области защиты информации
	НЗ-5 Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по

	защите информации
	НЗ-6 Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах
	НЗ-7 Принципы построения средств защиты информации от несанкционированного доступа и утечки по техническим каналам
	НЗ-8 Принципы построения и функционирования систем и сетей передачи информации