Приложение 1

Приложение к ОП

Паспорт компетенций, универсальных компетенций (УК) магистратуры ИБ

Код и наименование компетенции	Планируемые результаты обучения (индикаторы) [указываются в соответствии с содержанием трудовых функций из профессиональных стандартов (трудовыми действиями, необходимыми знаниями и умениями), соотносящимися с компетенцией]				**Модули и дисциплины**
	Знания:	**Умения:**	**Практический опыт, владение**	**Другие результаты** *(указываются при необходимости, к примеру,* ***личностные качества****)*	
УК-1 – Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	З-1 – Сделать обзор основных принципов критического мышления, методов анализа и оценки информации	У-1 – Осмысливать явления окружающего мира во взаимосвязи, целостности и развитии, выстраивать логические связи между элементами системы	П-1 – Выявлять и анализировать проблемную ситуацию, выделяя ее структурные составляющие и связи между ними		**Математические методы информационной безопасности** Математические методы теории сигналов и систем ГИА, практика
УК-2 – Способен управлять проектом на всех этапах его жизненного цикла	З-1 – Принципы формирования концепции проекта в рамках обозначенной проблемы; З-2 – Основные требования, предъявляемые к	У-1 – Разрабатывать концепцию проекта в рамках обозначенной проблемы, формулируя цель, задачи, актуальность, значимость (научную, практическую, методическую и иную в зависимости от типа	П-1 – навыками составления плана графика реализации проекта в целом и плана-контроля его выполнения; П-2 – навыками конструктивного преодоления		**Управление информационной безопасностью информационных систем персональных данных (ИСПДн), государственных информационных**

	проектной работе и критерии оценки результатов проектной деятельности;	проекта), ожидаемые результаты и возможные сферы их применения; У-2 – уметь видеть образ результата деятельности и планировать последовательность шагов для достижения данного результата; У-3 – прогнозировать проблемные ситуации и риски в проектной деятельности	возникающих разногласий и конфликтов.		**систем (ГИС) и значимых объектах критической информационной инфраструктуры (КИИ)** Управление проектами в области информационной безопасности ГИА, практика
УК-3 – Способен организовать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	З-1 — общие формы организации деятельности коллектива; З-2 — психологию межличностных отношений в группах разного возраста; З-3 — основы стратегического планирования работы коллектива для достижения поставленной цели;	У-1 — создавать в коллективе психологически безопасную доброжелательную среду; У-2 — учитывать в своей социальной и профессиональной деятельности интересы коллег; У-3 — предвидеть результаты (последствия) как личных, так и коллективных действий; У-4 — планировать командную работу, распределять поручения и делегировать полномочия членам команды;	П-1 — навыками постановки цели в условиях командой работы; П-2 — способами управления командной работой в решении поставленных задач; П-3 – навыками преодоления возникающих в коллективе разногласий, споров и конфликтов на основе учета интересов всех сторон.		**Управление информационной безопасностью информационных систем персональных данных (ИСПДн), государственных информационных систем (ГИС) и значимых объектах критической информационной инфраструктуры (КИИ)** Управление информационной безопасностью

					ИСПДн, ГИС и значимых объектов КИИ ГИА, практика
УК-4 — Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	З-1 — современные средства информационно-коммуникационных технологий; З-2 — языковой материал (лексические единицы и грамматические структуры), необходимый и достаточный для общения в различных средах и сферах речевой деятельности;	У-1 — воспринимать на слух и понимать содержание аутентичных общественно-политических, публицистических (медийных) и прагматических текстов, относящихся к различным типам речи, выделять в них значимую информацию; У-2 — понимать содержание научно-популярных и научных текстов, блогов/веб-сайтов; У-3 — выделять значимую информацию из прагматических текстов справочно-информационного и рекламного характера; У-4 — вести диалог, соблюдая нормы речевого этикета, используя различные стратегии; выстраивать монолог;	П-1 — практическими навыками использования современных коммуникативных технологий; П-2 – грамматическими категориями изучаемого (ых) иностранного (ых) языка (ов).		**Гуманитарные аспекты информационной безопасности** Профессиональный иностранный язык ГИА, практика

		У-5 — составлять деловые бумаги, в том числе оформлять CurriculumVitae/Resume и сопроводительное письмо, необходимые при приеме на работу; У-6 — вести запись основных мыслей и фактов (из аудиотекстов и текстов для чтения), запись тезисов устного выступления/письменного доклада по изучаемой проблеме; У-7 — поддерживать контакты при помощи электронной почты			
УК-5. Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	З-1 — различные исторические типы культур; З-2 — механизмы межкультурного взаимодействия в обществе на современном этапе, принципы соотношения общемировых и национальных культурных процессов;	У-1 — объяснить феномен культуры, её роль в человеческой жизнедеятельности; У-2 — адекватно оценивать межкультурные диалоги в современном обществе; У-3 — толерантно взаимодействовать с представителями различных культур.	П-1 — навыками формирования психологически-безопасной среды в профессиональной деятельности; П-2 — навыками межкультурного взаимодействия с учетом разнообразия культур.		**Гуманитарные аспекты информационной безопасности** Актуальные проблемы философии и истории науки ГИА, практика

УК-6. Способен определить и реализовать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки	З-1 — основы планирования профессиональной траектории с учетом особенностей как профессиональной, так и других видов деятельности и требований рынка труда;	У-1 — расставлять приоритеты профессиональной деятельности и способы ее совершенствования на основе самооценки; У-2 — планировать самостоятельную деятельность в решении профессиональных задач; У-3 — подвергать критическому анализу проделанную работу; У-4 — находить и творчески использовать имеющийся опыт в соответствии с задачами саморазвития;	П-1 — навыками выявления стимулов для саморазвития; П-2 — навыками определения реалистических целей профессионального роста.		**Гуманитарные аспекты информационной безопасности** Основы научного исследования ГИА, практика

Приложение 2

Приложение к ОП

Паспорт компетенций, универсальных компетенций (ОПК) магистратуры

Код и наименование компетенции	Планируемые результаты обучения (индикаторы) [указываются в соответствии с содержанием трудовых функций из профессиональных стандартов (трудовыми действиями, необходимыми знаниями и умениями), соотносящимися с компетенцией]				**Модули и дисциплины**
	Знания:	**Умения:**	**Практический опыт, владение**	**Другие результаты** *(указываются при необходимости, к примеру,*	

				личностные качества)	
ОПК-1 Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	З-1 - знать основы отечественных и зарубежных стандартов в области обеспечения информационной безопасности З-2 - знает направления развития и проблемы компьютерного моделирования сложных систем; направления развития технологий проектирования информационных, автоматизированных и автоматических систем. З-3 - знает современную нормативную базу и ГОСТы, регламентирующие процесс разработки ТЗ. Правила, способы и методы организации совместных разработок.	У-1 - уметь проектировать информационные системы с учетом различных технологий обеспечения информационной безопасности. У-2 - умеет обосновывать и планировать состав и архитектуру моделируемых сложных систем; обосновывать и планировать состав и архитектуру проектируемых информационных, автоматизированных и автоматических систем. У-3 – умеет формировать актуальную модель угроз для АИС и учитывать её положения при формировании требований ТЗ на	П-1 - владеть навыками участия в разработке системы обеспечения информационной безопасности объекта. П-2 - владеет навыками разработки концептуальных стратегий решения задач моделирования и проектирования автоматизированных информационных систем и систем обеспечения ИБ. П-3 – владеет навыками планирования и оценки трудоёмкости проекта, включая техническое, кадровое и финансовое обеспечение, принятие совместных решений.		**Защищенные информационные системы** Методология проектирования защищенных информационных систем ГИА, практика

	З-4 - знает методы проектирования и построения систем информационной безопасности, включая методы тестирования эффективности и оценки надёжности	проектируемую систему обеспечения ИБ. У-4 - умеет разрабатывать и обосновывать критерии оценки эффективности проектируемой системы обеспечения ИБ. Оценивать эффективность решений и анализировать показатели деятельности. У-5 - умеет обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности.			
ОПК-2. Способен разрабатывать технический проект системы (подсистемы либо	З-1 - знает методы концептуального проектирования технологий обеспечения	У-1 - умеет выбирать и обосновывать преимущества методов решения задач для защиты	П-1 - владеет навыками выполнения работы по осуществлению при изготовлении, монтаже, наладке, испытаниях и		**Защищенные информационные системы** Организация защищенных сетевых

компонента системы) обеспечения информационной безопасности	информационной безопасности. З-2 - знает направления развития и проблемы компьютерного моделирования сложных систем; направления развития технологий проектирования информационных, автоматизированных и автоматических систем. З-3 - знает современные методы и средства тестирования. З-4 - знать принципы построения и функционирования современных информационных систем. З-5 - знать назначение комплексной системы защиты информации, принципы ее организации и этапы разработки.	информации компьютерных систем и сетей и систем обеспечения информационной безопасностью. У-2 - умеет разрабатывать тестовые планы и сценарии тестирования разработанного продукта. У-3 - умеет управлять коллективом исполнителей и принимать управленческие решения. У-4 - уметь проектировать подсистемы безопасности информационных систем с учетом действующих нормативных и методических документов. У-5 - уметь разрабатывать модели угроз и	сдаче в эксплуатацию систем и средств обеспечения информационной безопасности. П-2 - владеет навыками практической реализации типовых задач разработки и исследования систем защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью. П-3 - владеет средствами автоматизированного и ручного функционального тестирования. П-4 - владеть навыками участия в организации комплексной системы защиты объекта.		коммуникаций в ИСПДн, ГИС и на объектах КИИ ГИА, практика

	З-6 - знать требования к системам комплексной защиты информации	нарушителей информационной безопасности информационных систем.			
ОПК-3. Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности	З-1 - знать основы отечественных и зарубежных стандартов в области сертификации и аттестации объектов информатизации, в области управления информационной безопасностью с целью разработки проектов организационно-распорядительных документов. З-2 - знать правила создания технического задания на создание подсистем безопасности информационных систем. З-3 - знать основные угрозы безопасности информации и модели нарушителя	У-1 - уметь разрабатывать технические задания на создание подсистем обеспечения информационной безопасности. У-2 - уметь проводить выбор, исследовать эффективность, проводить технико-экономическое обоснование проектных решений в области построения систем обеспечения информационной безопасности. У-3 - уметь разрабатывать проекты нормативных материалов, регламентирующих	П-1 - владеть навыками разработки политик безопасности различных уровней. П-2 - владеть навыками расчета и управления рисками информационной безопасности, навыками разработки положения о применимости механизмов контроля в контексте управления рисками информационной безопасности. П-3 - владеть правилами построения оптимальной политики безопасности в соответствии с требованиями уровня безопасности, стоимости и сроков реализации.		**Защищенные информационные системы** Защита информации в системах беспроводной связи ГИА, практика

	в информационных системах. З-4 - знать основные нормативные правовые акты в области обеспечения информационной безопасности. З-5 - знать нормативные методические документы ФСБ России в области защиты информации. З-6 - знать нормативные методические документы ФСТЭК России в области информационной безопасности.	работу по защите информации. У-4 - уметь разрабатывать нормативно-методические материалы по регламентации системы организационной защиты информации. У-5 - уметь разрабатывать организационно-распорядительную документацию по обеспечению информационной безопасности. У-6 - уметь работать с технической и эксплуатационной документацией. У-6 - уметь оценивать различные инструменты в области проектирования и управления информационной безопасности.	П-4 - владеть навыками работы с нормативными правовыми актами в области информационной безопасности.		

ОПК-4. Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок	З-1 - знать способы формулирования научной проблемы, гипотезы, выбора предмета, объекта, целей, задач исследования. З-2 - знать основные принципы создания эскизного, технического, рабочего проектов. З-3 - знать методы анализа и обоснования выбора решений по обеспечению требуемого уровня безопасности информационных систем. З-4 - знать современные достижения науки в области информационной безопасности. З-5 - знать правила, способы и методы организации, выполнения и представления результатов	У-1 - уметь составлять пошаговый план научной деятельности, проводить предпроектные исследования. У-2 - уметь работать с научной литературой, отбирать информацию по теме научного исследования, систематизировать, классифицировать полученную информацию. У-3 - уметь определять комплекс мер для обеспечения безопасности информационных систем, составлять аналитические обзоры по вопросам обеспечения информационной безопасности систем. У-4 - уметь использовать методы	П-1 - владеть навыками структурирования информации по теме исследования. П-2 - владеть навыками самостоятельного научного мышления, обобщения и систематизации информации. П-3 - владеть навыками сбора и обработки информации в глобальной компьютерной сети, в том числе в мультидисциплинарных реферативных базах данных Scopus, Web of Knowledge. П-4 - владеть методикой создания технического задания и технического проекта при организации НИОКР. П-5 - владеть программными и программно-аппаратными средствами анализа систем защиты информации.		**Математические методы информационной безопасности** Методы и инструменты анализа больших данных Гуманитарные аспекты информационной безопасности Основы научного исследования, Правовые аспекты информационной безопасности ИСПДн, ГИС и значимых объектов КИИ ГИА, практика

	научного исследования. З-6 - знать о правилах и стандартах разработки отчетной документации. З-7 - знать основные категории и понятия информационно аналитической работы, принципы и методы ее ведения. З-8 - знать методы выработки и принятия информационного решения. З-9 - знать технологии поиска, изучения, обобщения и систематизации научной информации. З-10 - знать виды отчетно-информационных документов, методы их подготовки. З-11 - знать основные теоретико-числовые методы	и средства анализа защищенности информационных систем. У-5 - уметь использовать программные и аппаратные средства персонального компьютера для поиска и обработки информации. У-6 - уметь разрабатывать планы и программы проведения научных исследований в соответствии с техническим заданием, ресурсным обеспечением и заданными сроками выполнения работы. У-7 - уметь представлять результаты научно-исследовательской деятельности в виде презентаций, отчетов, устных докладов. У-8 - уметь логически мыслить,	П-6 - владеть навыками поиска информации в глобальной информационной сети Интернет. П-7 - владеть методологией научных исследований в сфере информационной безопасности. П-8 - владеть навыками планирования научного исследования. П-9 - владеть основными методами поиска и структурирования информации.		

	применительно к задачам защиты информации.	вести научные дискуссии. У-9 - уметь использовать справочную и научную литературу по тематике решаемых информационных задач, оценивать специальную информацию, систематизировать ее, принимать решение о ее дальнейшем использовании.			
ОПК-5. Способен проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований	З-1 - знать теоретические и эмпирические методы научных исследований. З-2 - знать порядок проведения научных исследований. З-3 - знать методику проведения патентных исследований, объектом которых могут являться объекты техники,	У-1 - уметь применять методы научных исследований в научной деятельности, в частности, при написании магистерской диссертации и научных статей. У-2 - уметь составлять отчеты о патентных	П-1 - владеть навыками оформления научных публикаций в соответствие с шаблоном IEEE, требованиями научных конференций. П-2 - владеть теоретическими и эмпирическими методами научного исследования при выполнении научно-исследовательских работ.		**Математические методы информационной безопасности** Безопасность автоматизированных информационно-управляющих систем Математические методы теории сигналов и систем Методы и инструменты

научные доклады и статьи	промышленной и интеллектуальной собственности (изобретения, полезные модели, программы для ЭВМ и базы данных и др.), ноу-хау и пр. З-4 - знает порядок организации процесса исследования эффективности системы управления ИБ. З-4 - знать нормативные и методические материалы в сфере информационной безопасности. З-5 - знать принципы организации технического, программного и информационного обеспечения информационной безопасности. З-6 - знать методы построения оптимальных планов	исследованиях по ГОСТ. У-3 - умеет формализовать задачи анализа безопасности информационных систем, разрабатывать методики исследования и применять инструментальные средства анализа безопасности. У-4 - уметь составлять и корректировать план проведения работ в зависимости от полученных результатов. У-5 - уметь оформлять и представлять результаты, полученные в ходе выполнения научно-исследовательского проекта грамотно, лаконично, в достаточном объеме	П-3 - владеть методикой оформления отчетов по научно-исследовательским работам согласно ГОСТ. П-4 - владеет навыками выбора и обоснования критериев оценки защищенности открытых информационных систем. П-5 - владеет навыками обработки, оценки и представления результатов исследования эффективности решений по управлению информационной безопасностью. П-6 - владеть навыками разработки технической документации в соответствии с требованиями Единой системы конструкторской документации и Единой системы программной документации.		анализа больших данных Специальные разделы математики ГИА, практика

	для научных экспериментов. З-7 - знать правила, способы и методы организации, выполнения и представления результатов научного исследования. З-8 - знать принципы построения и функционирования современных информационных систем. З-9 - знать основные элементы научно-технического эксперимента. З-10 - знать приемы выбора основных факторов эксперимента и технологию построения факторных планов. З-11 - знать требования ГОСТов на оформление научно-технической документации.	на русском и иностранном языках. У-6 - уметь выбирать и применять в профессиональной деятельности экспериментальные и расчетно-теоретические методы исследований. У-7 - уметь работать со специальными программными средствами для оформления проектной и отчетной документации. У-8 - уметь обобщать полученные экспериментальные данные, анализировать и делать выводы.	П-7 - владеть навыками анализа получаемых результатов и формулировки выводов. П-8 - владеть навыками формирования и аргументированного обоснования собственной позиции по различным проблемам защиты информации. П-9 - владеть навыками представления результатов работы в виде презентаций, пояснительных записок, научных докладов и статей. П-10 - владеть навыками самостоятельной работы, самоорганизации.		

	З-12 - знать современные модели и методы измерения, прогнозирования, принятия решений при решении практических задач. З-13 - знать принципы построения вероятностных моделей применительно к практическим задачам.				

Приложение 3

Приложение к ОП

Паспорт компетенций, универсальных компетенций (ПК) магистратуры

Код и наименование компетенции	Планируемые результаты обучения (индикаторы) [указываются в соответствии с содержанием трудовых функций из профессиональных стандартов (трудовыми действиями, необходимыми знаниями и умениями), соотносящимися с компетенцией]				**Модули и дисциплины**
	Знания:	**Умения:**	**Практический опыт, владение**	**Другие результаты** *(указываются при необходимости, к примеру,* ***личностные качества)***	
ПК 1. Способен решать типовые задачи анализа информации в ИАС государственных органов обеспечивающих национальную безопасность.	З-1 Методологические основы теории принятия решений, теории измерений, теории прогнозирования и планирования З-2 Способы измерения свойств объектов предметной области З-3	У-1 Проверять гипотезы и границы их применения в задачах анализа информации в ИАС У-2 Разрабатывать и применять математические модели и методы решения задач анализа информации в ИАС, создавая	П-1 Выдвижение гипотез, определение границ их применения и подтверждение или опровержение их на практике П-2 Решение типовых задач анализа информации в ИАС П-3		Методы и средства защиты информации в информационных системах персональных данных (ИСПДн), государственных информационных системах (ГИС) и значимых объектах критической информационной инфраструктуры (КИИ)

	Методы теории вероятностей, теории случайных процессов и математической статистики З-4 Математические модели, методы и алгоритмы решения типовых задач анализа информации в ИАС З-5 Программное обеспечение процесса решения задач анализа информации в ИАС З-6 Методические подходы к интерпретации профессионального смысла получаемых результатов анализа информации в ИАС З-7 Методы оценки эффективности и	соответствующее программное и математическое обеспечение У-3 Строить алгоритмы решения типовых задач анализа информации в ИАС и создавать программы их реализации У-4 Представлять результаты решения аналитических задач в стандартном виде У-5 Интерпретировать профессиональный смысл получаемых результатов анализа информации в ИАС	Интерпретация профессионального смысла получаемых формальных результатов		Меры и средства защиты информации от несанкционированного доступа в ИСПДн, ГИС и значимых объектах КИИ Методы контроля защищенности информации ИСПДн, ГИС и значимых объектов КИИ Стандарты и методы оценки защищенности ИСПДн, ГИС и значимых объектов КИИ ГИА, практика

	качества в задачах прогнозирования, планирования, принятия решений при различной априорной неопределенности имеющейся информации З-8 Нормативные правовые акты в области защиты информации З-9 Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации З-10 Организационные меры по защите информации				
ПК 2. Способен проводить анализ безопасности	З-1 Принципы построения	У-1 Анализировать компьютерную	П-1 Определение уровня защищенности и		**Криптографические методы защиты информации**

компьютерных систем.	компьютерных систем и сетей З-2 Уязвимости компьютерных систем и сетей З-3 Криптографические методы защиты информации З-4 Принципы построения систем управления базами данных З-5 Средства анализа конфигураций З-6 Национальные, межгосударственные и международные стандарты в области защиты информации З-7 Нормативные правовые акты в	систему с целью определения уровня защищенности и доверия У-2 Прогнозировать возможные пути развития действий нарушителя информационной безопасности У-3 Производить анализ политики безопасности на предмет адекватности У-4 Проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в операционных системах У-5 Составлять и оформлять	доверия в компьютерных системах П-2 Оценка рисков, связанных с осуществлением угроз безопасности в отношении компьютерных систем П-3 Оценка соответствия механизмов безопасности компьютерной системы требованиям существующих нормативных документов, а также их адекватности существующим рискам П-4 Подготовка аналитического отчета по результатам проведенного анализа П-5		Криптографические алгоритмы и протоколы Криптографические методы и средства защиты в ИСПДн, ГИС и значимых объектах КИИ ГИА, практика

	области защиты информации З-8 Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации З-9 Организационные меры по защите информации	аналитический отчет по результатам проведенного анализа У-6 Разрабатывать предложения по устранению выявленных уязвимостей	Формулирование предложений по устранению выявленных уязвимостей		
ПК 3. Способен проводить экспертизу при расследовании компьютерных преступлений, правонарушений и инцидентов.	З-1 Принципы построения компьютерных систем и сетей З-2 Уязвимости компьютерных систем и сетей З-3 Криптографические методы защиты информации	У-1 Анализировать компьютерную систему с целью определения уровня защищенности и доверия У-2 Прогнозировать возможные пути развития действий нарушителя информационной безопасности	П-1 Определение уровня защищенности и доверия в компьютерных системах П-2 Оценка рисков, связанных с осуществлением угроз безопасности в отношении компьютерных систем П-3		Организация и функционирование центров мониторинга Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА) Анализ событий безопасности и обеспечение функционирования

	З-4 Принципы построения систем управления базами данных З-5 Средства анализа конфигураций З-6 Национальные, межгосударственные и международные стандарты в области защиты информации З-7 Нормативные правовые акты в области защиты информации З-8 Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации	У-3 Производить анализ политики безопасности на предмет адекватности У-4 Проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в операционных системах У-5 Составлять и оформлять аналитический отчет по результатам проведенного анализа У-6 Разрабатывать предложения по устранению выявленных уязвимостей	Оценка соответствия механизмов безопасности компьютерной системы требованиям существующих нормативных документов, а также их адекватности существующим рискам П-4 Подготовка аналитического отчета по результатам проведенного анализа П-5 Формулирование предложений по устранению выявленных уязвимостей		технических средств сегмента ГосСОПКА Реагирование и ликвидация последствий компьютерных инцидентов в рамках функционирования центров мониторинга ГосСОПКА Экспертно-аналитическая деятельность в центрах мониторинга ГосСОПКА Обнаружение и предупреждение компьютерных атак на объектах критической информационной инфраструктуры (КИИ) Реагирование на компьютерные инциденты, ликвидация их последствий на объектах КИИ Экспертная и аналитическая деятельность в сфере обеспечения

	З-9 Организационные меры по защите информации				безопасности объектов КИИ Эксплуатация систем обнаружения компьютерных атак на объектах КИИ ГИА, практика
ПК 4. Способен разрабатывать программные и программно-аппаратные средства для систем защиты информации автоматизированных систем.	З-1 Профессиональная и криптографическая терминология в области безопасности информации З-2 Основные информационные технологии, используемые в автоматизированных системах З-3 Средства и способы обеспечения безопасности информации, принципы построения систем защиты информации З-4	У-1 Оценивать сложность алгоритмов и вычислений У-2 Разрабатывать технические задания на создание подсистем безопасности информации автоматизированных систем, проектировать такие подсистемы с учетом требований нормативных документов, ЕСКД и ЕСПД У-3 Анализировать программные, архитектурно-технические и схемотехнические	П-1 Разработка технической документации в соответствии с требованиями Единой системы конструкторской документации (ЕСКД) и Единой системы программной документации (ЕСПД) на компоненты автоматизированных систем П-2 Применение средств схемотехнического проектирования и современной измерительной аппаратуры П-3		Обнаружение и предупреждение компьютерных атак на объектах критической информационной инфраструктуры (КИИ) Реагирование на компьютерные инциденты, ликвидация их последствий на объектах КИИ Экспертная и аналитическая деятельность в сфере обеспечения безопасности объектов КИИ ГИА, практика

	Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах З-5 Современные технологии программирования З-6 Эталонная модель взаимодействия открытых систем, основные протоколы, последовательность и содержание этапов построения и функционирования современных локальных и глобальных компьютерных сетей З-7 Особенности защиты информации в автоматизированных системах управления	решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах У-4 Проводить комплексное тестирование аппаратных и программных средств	Синтез структурных и функциональных схем защищенных автоматизированных систем П-4 Разработка программного обеспечения, технических средств, баз данных и компьютерных сетей с учетом требований по обеспечению защиты информации П-5 Разработка электронных схем с учетом требований по защите информации П-6 Оптимизация работы электронных схем с учетом требований по защите информации		

	технологическими процессами З-8 Принципы работы элементов и функциональных узлов электронной аппаратуры, типовые схемотехнические решения основных узлов и блоков электронной аппаратуры З-9 Принципы организации документирования разработки и процесса сопровождения программного и аппаратного обеспечения З-10 Методы тестирования и отладки программного и аппаратного обеспечения З-11				

	Архитектура, основные модели, последовательность и содержание этапов проектирования, физическая организация баз данных З-12 Нормативные правовые акты в области защиты информации З-13 Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации				
ПК 5. Способен разработать и смоделировать программно-технические средства защиты информации от несанкционированного доступа	З-1 Нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного	У-1 Разрабатывать техническое задание на создание программно-технического средства защиты информации от несанкционированног	П-1 Разработка технического задания на создание программно-технического средства защиты информации от несанкционированног		**Методы и средства защиты информации в информационных системах персональных данных (ИСПДн), государственных информационных системах (ГИС) и**

	доступа, проектирования средств защиты информации, сертификации средств защиты информации на соответствие требованиям по безопасности информации и аттестации объектов информатизации на соответствие требованиям по защите информации З-2 Стандарты ЕСКД, ЕСТД и ЕСПД З-3 Современные информационные технологии (операционные системы, базы данных, вычислительные сети) З-4 Способы реализации несанкционированного доступа к	о доступа и специальных воздействий на нее У-2 Разрабатывать проектно-сметную документацию на создание программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее У-3 Проектировать с использованием современных программных средств проектирования программно-техническое средство защиты информации от несанкционированного доступа и специальных воздействий на нее У-4	о доступа и специальных воздействий на нее П-2 Разработка проектно-сметной документации на создание программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее П-3 Разработка предварительных проектных решений по созданию программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее П-4		**значимых объектах критической информационной инфраструктуры (КИИ)** Меры и средства защиты информации от несанкционированного доступа в ИСПДн, ГИС и значимых объектах КИИ Методы контроля защищенности информации ИСПДн, ГИС и значимых объектов КИИ Стандарты и методы оценки защищенности ИСПДн, ГИС и значимых объектов КИИ ГИА, практика

	информации и специальных программных воздействий на информацию и ее носители в автоматизированных системах З-5 Основные классы и виды уязвимостей программного обеспечения З-6 Методы и технологии защиты информации от несанкционированного доступа и специальных программных воздействий на нее З-7 Программные (программно-технические) средства защиты автоматизированных систем от несанкционированног	Разрабатывать конструкторскую, технологическую и эксплуатационную документацию по правилам, установленным стандартами ЕСКД, ЕСТД и ЕСПД У-5 Изготавливать опытный образец программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее У-6 Разрабатывать программы и методики испытаний программно-технического средства защиты информации от несанкционированного доступа и	Разработка технического (эскизного) проекта программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее П-5 Разработка конструкторской и технологической документации на программное (программно-техническое) средство защиты информации от несанкционированного доступа и специальных воздействий на нее по правилам, установленным стандартами ЕСКД, ЕСТД и ЕСПД П-6		

	о доступа к информации и специальных программных воздействий на нее З-8 Методы контроля защищенности информации от несанкционированного доступа и специальных программных воздействий З-9 Средства контроля защищенности информации от несанкционированного доступа З-10 Методики контроля защищенности информации от несанкционированного доступа З-11	специальных воздействий на нее У-7 Проводить испытания программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее	Изготовление опытного образца программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее П-7 Разработка программы и методик испытаний программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее П-8 Испытания программно-технического средства защиты информации от несанкционированного доступа и		

	Средства проектирования электронных схем З-12 Языки и современные технологии программирования З-13 Технологии производства электронной аппаратуры		специальных воздействий на нее П-9 Разработка рабочей и эксплуатационной документации на техническое средство защиты П-10 информации от несанкционированного доступа и специальных воздействий на нее		