Минобрнауки России

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Сыктывкарский государственный университет им. Питирима Сорокина»

(ФГБОУ ВО «СГУ им. Питирима Сорокина»)

УТВЕРЖДЕНА
решением Ученого совета
от «28» марта 2024 г. № 1/13 (610)

ОСНОВНАЯ ПРОФЕССИОНАЛЬНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА ВЫСШЕГО ОБРАЗОВАНИЯ

по специальности

10.05.03 Информационная безопасность автоматизированных систем

Направленность (профиль) программы –

специализация №7 «Анализ безопасности информационных систем»

Присваиваемая квалификация –

Специалист по защите информации

Китайгородский Михаил Дмитриевич

Подписано цифровой подписью: Китайгородский Михаил Дмитриевич
Дата: 2024.06.10 12:17:58 +03'00'

Сыктывкар
2024

СОДЕРЖАНИЕ

1. Общие положения

1.1. Основная профессиональная образовательная программа (далее – ОПОП) сформирована в соответствии с законодательством Российской Федерации, в том числе с Федеральным государственным образовательным стандартом высшего образования по специальности 10.05.03 Информационная безопасность автоматизированных систем (далее – ФГОС ВО) (утв. приказом Минобрнауки России от 26.11.2020 № 1457), с учетом профессиональных стандартов «Специалист по безопасности компьютерных систем и сетей» (утв. приказом Минтруда России от 14.09.2022 № 533н), «Специалист по защите информации в автоматизированных системах» (утв. приказом Минтруда России от 14.09.2022 № 525н), «Специалист по технической защите информации» (утв. приказом Минтруда России от 09.08.2022 № 474н).

1.2. Обучение по ОПОП может осуществляться в очной форме обучения.

1.3. Сроки обучения:

– по очной форме – 5,5 лет;

– при обучении по индивидуальному учебному плану устанавливается Университетом, но не более срока получения образования, установленного для соответствующей формы обучения;

– при обучении по индивидуальному плану лиц с ограниченными возможностями здоровья Университет вправе продлить срок не более чем на один год по сравнению со сроком, установленным для соответствующей формы обучения.

1.4. Объем ОПОП составляет 330 зачетных единиц (далее – з.е.) вне зависимости от формы обучения, применяемых образовательных технологий, реализации ОПОП по индивидуальному учебному плану.

Объем контактной работы определяется требованиями ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем, локальными актами университета, а также учебным планом в части контактной работы при проведении учебных занятий и составляет в очной форме обучения - не менее 50 процентов объема программы специалитета, отводимого на реализацию дисциплин (модулей).

1.5. Образовательная деятельность по ОПОП осуществляется на государственном языке Российской Федерации.

1.6. ОПОП может быть частично реализована с применением электронного обучения, дистанционных образовательных технологий.

1.7. Образовательная деятельность по ОПОП при реализации части учебных предметов, курсов, дисциплин (модулей), практик, иных компонентов образовательных

программ, предусмотренных учебным планом, организуется в форме практической подготовки.

2. Характеристика профессиональной деятельности выпускника

2.1. Область профессиональной деятельности и сферы профессиональной деятельности выпускника по ОПОП:

06 Связь, информационные и коммуникационные технологии (в сфере обеспечения безопасности информации в автоматизированных системах).

2.2. Типы задач профессиональной деятельности выпускника по ОПОП:

– научно-исследовательский;

– проектный;

– контрольно-аналитический;

– организационно-управленческий;

– эксплуатационный.

2.3. Перечень основных задач профессиональной деятельности выпускников.

Основные задачи профессиональной деятельности определяются требованиями ФГОС ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем, профилем (направленностью) ОПОП – специализация N 7 «Анализ безопасности информационных систем» и требованиями профессиональных стандартов «Специалист по безопасности компьютерных систем и сетей», «Специалист по защите информации в автоматизированных системах», «Специалист по технической защите информации» (таблица 1).

Таблица 1. Задачи профессиональной деятельности

Область профессиональной деятельности (по Реестру Минтруда)	*Типы задач профессиональной деятельности*	*Задачи профессиональной деятельности*	*Объекты профессиональной деятельности (или области знания)*
«Специалист по защите информации в автоматизированных системах»			
06 Связь, информационные и коммуникационные технологии	научно-исследовательский	сбор, обработка, анализ и систематизация научно-технической информации по проблематике информационной безопасности автоматизированных систем; подготовка научно-технических отчетов, обзоров, докладов, публикаций по результатам	автоматизированные системы, функционирующие в условиях существования угроз в информационной сфере и обладающие информационно-технологическими ресурсами, подлежащими защите; информационные

		выполненных исследований; моделирование и исследование свойств защищенных автоматизированных систем, разработка модели угроз и модели нарушителя информационной безопасности, методик и тестов для анализа степени защищенности информационной системы и ее соответствия нормативным требованиям по защите информации; анализ защищенности информации в автоматизированных системах и безопасности реализуемых информационных технологий; разработка эффективных решений по обеспечению информационной безопасности автоматизированных систем.	технологии, формирующие информационную инфраструктуру в условиях существования угроз в информационной сфере и задействующие информационно-технологические ресурсы, подлежащие защите; технологии обеспечения информационной безопасности автоматизированных систем.
	проектный	сбор и анализ исходных данных для проектирования защищенных автоматизированных систем; разработка политик информационной безопасности автоматизированных систем; разработка защищенных автоматизированных систем в сфере профессиональной деятельности, обоснование выбора способов и средств защиты информационно-технологических ресурсов автоматизированных систем; выполнение проектов по созданию программ, комплексов программ, программно-аппаратных средств, баз данных, компьютерных сетей для защищенных автоматизированных систем;	автоматизированные системы, функционирующие в условиях существования угроз в информационной сфере и обладающие информационно-технологическими ресурсами, подлежащими защите; системы управления информационной безопасностью автоматизированных систем.

		разработка систем управления информационной безопасностью автоматизированных систем.	
«Специалист по технической защите информации»			
06 Связь, информационные и коммуникационные технологии	контрольно-аналитический	контроль работоспособности и эффективности применяемых средств защиты информации; выполнение экспериментально-исследовательских работ при сертификации средств защиты информации и аттестации автоматизированных систем; проведение инструментального мониторинга защищенности автоматизированных систем и анализа его результатов.	автоматизированные системы, функционирующие в условиях существования угроз в информационной сфере и обладающие информационно-технологическими ресурсами, подлежащими защите.
	организационно-управленческий	организация работы коллектива, принятие управленческих решений в условиях спектра мнений, определение порядка выполнения работ; организационно-методическое обеспечение информационной безопасности автоматизированных систем; организация работ по созданию, внедрению, эксплуатации и сопровождению защищенных автоматизированных систем; контроль реализации политики информационной безопасности.	автоматизированные системы, функционирующие в условиях существования угроз в информационной сфере и обладающие информационно-технологическими ресурсами, подлежащими защите; системы управления информационной безопасностью автоматизированных систем.
«Специалист по безопасности компьютерных систем и сетей»			
06 Связь, информационные и коммуникационные технологии	эксплуатационный	реализация информационных технологий в сфере профессиональной деятельности с использованием защищенных автоматизированных	информационные технологии, формирующие информационную инфраструктуру в условиях существования угроз в информационной

		систем; мониторинг информационной безопасности автоматизированных систем; управление информационной безопасностью автоматизированных систем; обеспечение восстановления работоспособности систем защиты информации при возникновении нештатных ситуаций.	сфере и задействующие информационно-технологические ресурсы, подлежащие защите; технологии обеспечения информационной безопасности автоматизированных систем.

3. Результаты освоения образовательной программы

3.1. В результате освоения образовательной программы у выпускника должны быть сформированы универсальные (таблица 2), общепрофессиональные (таблица 3) и профессиональные компетенции (таблица 4). Результаты сформированности компетенций определяются индикаторами их достижения.

Таблица 2. Универсальные компетенции и индикаторы их достижения

Наименование категории (группы) универсальных компетенций	*Код и наименование универсальной компетенции выпускника*	*Код и наименование индикатора достижения универсальной компетенции*
Системное и критическое мышление	УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.1. Анализирует проблемную ситуацию с применением системного подхода и современного социально-научного знания, используя достоверные данные и надежные источники информации. УК-1.2. Разрабатывает и содержательно аргументирует возможные стратегии решения проблемной ситуации на основе системного и междисциплинарного подходов с учетом параметров социокультурной среды. УК-1.3. Разрабатывает сценарий реализации оптимальной стратегии решения проблемной ситуации с учетом необходимых ресурсов, достижимых результатов, возможных рисков и последствий.
Разработка и реализация проектов	УК-2. Способен управлять проектом на всех этапах его жизненного цикла	УК-2.1. Разрабатывает концепцию проекта в рамках конкретного проблемного поля с учетом возможных результатов и последствий реализации проекта в конкретной социокультурной среде, теоретически обосновывает

		концепцию. УК-2.2. Разрабатывает план реализации проекта с учетом возможных ресурсов, рисков, сценариев, других вариативных параметров, предлагает процедуры и механизмы мониторинга реализации и результатов проекта. УК-2.3. Осуществляет координацию и контроль в процессе реализации проекта, корректирует отклонения, вносит дополнительные изменения в план реализации в случае необходимости, определяет зоны ответственности членов команды.
Командная работа и лидерство	УК-3. Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	УК-3.1. Вырабатывает стратегию командной работы для достижения поставленной цели, организует отбор участников команды. УК-3.2. Организует и корректирует работу команды, в том числе на основе коллегиальных решений, распределяет функциональные обязанности, разрешает возможные конфликты и противоречия. УК-3.3. Координирует общую работу, организует обратную связь, контролирует результат, принимает управленческую ответственность.
Коммуникация	УК-4. Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	УК-4.1. Создает различные типы письменных и устных текстов на русском и иностранном языке для академического и профессионального взаимодействия. УК-4.2. Участвует в процессах профессиональной коммуникации на русском и иностранном языке, в том числе с применением современных коммуникативных технологий. УК-4.3. Представляет результаты исследовательской и проектной деятельности на различных публичных мероприятиях, участвует в академических и профессиональных дискуссиях на иностранном языке.
Межкультурное взаимодействие	УК-5. Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	УК-5.1. Анализирует социокультурные параметры различных групп и общностей и социокультурный контекст взаимодействия. УК-5.2. Выстраивает социокультурную коммуникацию и взаимодействие с учетом необходимых параметров межкультурной коммуникации и социокультурного контекста. УК-5.3. Выстраивает профессиональное взаимодействие в мультикультурной среде.
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. Определяет приоритеты собственной деятельности, оценивает собственные ресурсы (личностные временные и др.) и их пределы, целесообразно их использует с учетом параметров социокультурной среды. УК-6.2. Определяет траекторию

		личного и профессионального саморазвития и инструменты целедостижения, в том числе образовательные (самообразование, повышения квалификации, пере-подготовка и др.) УК-6.3. Выстраивает гибкую профессиональную траекторию с учетом накопленного опыта профессиональной деятельности, изменяющихся требований рынка труда, стратегии личностного развития.
	УК-7. Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности	УК-7.1. Знает основы здорового образа жизни, здоровье-сберегающих технологий, физической культуры. УК-7.2. Умеет выполнять комплекс физкультурных упражнений. УК-7.3. Имеет практический опыт занятий физической культурой.
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 ситуаций и военных конфликтов	УК-8.1. Знает основы безопасности жизнедеятельности, телефоны служб спасения. УК-8.2. Умеет оказать первую помощь в чрезвычайных ситуациях, создавать безопасные условия реализации профессиональной деятельности. УК-8.3. Владеет навыками поддержания безопасных условий жизнедеятельности.
Экономическая культура, в том числе финансовая грамотность	УК-9. Способен принимать обоснованные экономические решения в различных областях жизнедеятельности	УК-9.1. Знает и понимает базовые принципы функционирования экономики и экономического развития, цели и формы участия государства в экономике. УК-9.2. Умеет применять методы личного экономического и финансового планирования для достижения текущих и долгосрочных финансовых целей, использует финансовые инструменты для управления личными финансами (личным бюджетом), контролирует собственные экономические и финансовые риски. УК-9.3. Владеет инструментами управления личными финансами для достижения поставленных финансовых целей.
Гражданская позиция	УК-10. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	УК-10.1. Иметь представление о понятии и сущности экстремизма, терроризма, коррупции; формах их проявления в современном обществе; их общественной опасности; основы системы противодействия этим явлениям в России, в том числе базовые положения предметного российского законодательства, основные виды правонарушений экстремистского, террористического, коррупционного характера, виды и меры юридической ответственности за их совершение; о необходимости противодействия экстремистским, террористическим,

		коррупционным проявлениям. УК-10.2. Уметь определять признаки экстремистской, террористической, коррупционной деятельности и давать им правовую оценку; идентифицировать конкретные органы публичной власти и иные субъекты, в компетенцию которых входит противодействие различным формам проявления указанных деструктивных социальных явлений; использовать систему мер противодействия экстремистским, террористическим и коррупционным проявлениям в области своей профессиональной деятельности. УК-10.3. Владеть навыками реализации правовых актов в области противодействия экстремистским, террористическим и коррупционным проявлениям в сфере профессиональной деятельности.

Таблица 3. Общепрофессиональные компетенции и индикаторы их достижения

Код и наименование общепрофессиональной компетенции	*Код и наименование индикатора достижения общепрофессиональной компетенции*
ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства.	ОПК-1.1. Знает основные понятия информатики; назначение, функции и структуру операционных систем, вычислительных сетей и систем управления базами данных. ОПК-1.2. Умеет использовать программные и аппаратные средства персонального компьютера; применять программные средства системного, прикладного и специального назначения. ОПК-1.3. Владеет навыками поиска информации в глобальной информационной сети Интернет и работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов, СУБД и т.п.); навыками обеспечивать работоспособности операционных систем и прикладных программ
ОПК-2. Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности.	ОПК-2.1. Знает основные программные средства системного и прикладного назначения, в том числе отечественного производства и методы использования. ОПК-2.1. Умеет применять программные средства системного и прикладного назначения, в том числе отечественного производства. ОПК-2.1. Владеет навыками решения задач профессиональной деятельности с использованием программных средств системного и прикладного назначения, в том числе отечественного производства.
ОПК-3. Способен использовать математические методы, необходимые для решения задач профессиональной деятельности.	ОПК-3.1. Знает необходимые математические методы. ОПК-3.2. Умеет определять и применять необходимые математические методы. ОПК-3.3. Владеет навыками решения задач профессиональной деятельности с использованием необходимые математические методы.
ОПК-4. Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические	ОПК-4.1. Знает физические законы и модели, в так же явления и процессы, лежащие в основе функционирования микроэлектронной техники. ОПК-4.2. Умеет определять и применять необходимые физические законы и модели при решении задач профессиональной деятельности.

законы и модели для решения задач профессиональной деятельности.	ОПК-4.3. Владеет навыками решения задач профессиональной деятельности с использованием необходимых физических законов и моделей.
ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации.	ОПК-5.1. Знает основы организационного и правового обеспечения информационной безопасности; основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации; основные нормативные правовые акты в области информационной безопасности и защиты информации. ОПК-5.2. Умеет применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; пользоваться нормативными документами по защите информации. ОПК-5.3. Владеет навыками работы с нормативными правовыми актами; навыками работы с нормативными правовыми актами по защите информации.
ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.	ОПК-6.1. Знает правовые основы организации защиты государственной тайны и конфиденциальной информации; задачи органов защиты государственной тайны и служб защиты информации на предприятиях; организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации; нормативные методические документы ФСБ России, ФСТЭК России в области защиты информации. ОПК-6.2. Умеет пользоваться нормативными документами ФСБ России и ФСТЭК России в области защиты информации. ОПК-6.3. Владеет навыками организации и обеспечения режима коммерческой тайны и/или режима секретности.
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.	ОПК-7.1. Знает современные средства разработки и анализа программного обеспечения на языках высокого уровня; методы программирования и методы разработки эффективных алгоритмов решения прикладных задач. ОПК-7.2. Умеет выбирать необходимые инструментальные средства для разработки программ в различных операционных системах и средах; составлять, тестировать, отлаживать и оформлять программы на языках высокого уровня, включая объектно-ориентированные. ОПК-7.3. Владеет навыками разработки программ на языке программирования высокого уровня; основными подходами к организации процесса разработки программного обеспечения.
ОПК-8. Способен применять методы научных исследований при проведении разработок в области защиты информации в автоматизированных системах.	ОПК-8.1. Знает основные методы поиска информации по ключевым словам; основные источники информации по вопросам обеспечения информационной безопасности автоматизированных систем. ОПК-8.2. Умеет осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по профилю своей деятельности; составлять обзор по вопросам обеспечения информационной безопасности автоматизированных систем. ОПК-8.3. Владеет навыками представления результатов научных исследований по вопросам обеспечения информационной безопасности по профилю своей деятельности с использованием современных технических средств в устной и письменной формах.
ОПК-9. Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты	ОПК-9.1. Знает современные информационные технологии и средства технической защиты информации, сетей и систем передачи информации, основные тенденции их развития. ОПК-9.2. Умеет выявлять тенденции развития информационных технологий. ОПК-9.2. Владеет навыками решения задач профессиональной

информации, сетей и систем передачи информации.	деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации.
ОПК-10. Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности.	ОПК-10.1. Знает современные средства криптографической и технической защиты информации. ОПК-10.2. Умеет использовать и настраивать современные средства криптографической и технической защиты информации. ОПК-10.3. Владеет навыками решения задач профессиональной деятельности с использованием современных средства криптографической и технической защиты информации.
ОПК-11. Способен разрабатывать компоненты систем защиты информации автоматизированных систем.	ОПК-11.1. Знает структуру систем защиты информации автоматизированных систем. ОПК-11.1. Умеет выявлять основные компоненты системы защиты информации автоматизированных систем. ОПК-11.2. Владеет навыками разработки компонентов систем защиты информации автоматизированных систем.
ОПК-12. Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем.	ОПК-12.1. Знает основные подходы к обеспечению безопасности вычислительных сетей, операционных систем и баз данных. ОПК-12.2. Умеет настраивать компоненты и средства защиты информации для вычислительных сетей, операционных систем и баз данных. ОПК-12.3. Владеет навыками обеспечения безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем.
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 методы диагностики и тестирования систем защиты информации автоматизированных систем, методы анализа уязвимостей систем защиты информации автоматизированных систем. ОПК-13.2. Умеет применять средства диагностики и тестирования систем защиты информации автоматизированных систем, средства анализа уязвимостей систем защиты информации автоматизированных систем. ОПК-13.3. Владеет навыками диагностики и тестирования систем защиты информации автоматизированных систем, способен проводить анализ уязвимостей систем защиты информации автоматизированных систем.
ОПК-14. Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений.	ОПК-14.1. Знает требования законодательства к защите информации в автоматизированных системах. ОПК-14.2. Умеет проводить подготовку исходных данных для технико-экономического обоснования проектных решений для систем защиты информации в автоматизированных системах. ОПК-14.3. Владеет навыками разработки, внедрения и эксплуатации автоматизированных систем в защищённом исполнении с учетом требований по защите информации.
ОПК-15. Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем.	ОПК-15.1. Знает методы администрирования и контроля функционирования средств и систем защиты информации автоматизированных систем, методы инструментального мониторинга защищенности автоматизированных систем. ОПК-15.1. Умеет применять средства администрирования и контроля функционирования средств и систем защиты информации автоматизированных систем, применять средства инструментального мониторинга защищенности автоматизированных систем. ОПК-15.3. Владеет навыками администрирования и контроля функционирования средств и систем защиты информации автоматизированных систем, навыками инструментального мониторинга защищенности автоматизированных систем.
ОПК-16. Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей	ОПК-16.1. Знает основные закономерности исторического процесса; этапы исторического развития России, место и роль России в истории человечества и в современном мире; ключевые события истории России и мира с древности до наших дней,

истории, в том числе для формирования гражданской позиции и развития патриотизма.	выдающихся деятелей отечественной истории; различные оценки и периодизации Отечественной истории. ОПК-16.2. Умеет соотносить общие исторические процессы и отдельные факты, выявлять существенные черты исторических процессов, явлений и событий; извлекать уроки из исторических событий и на их основе принимать осознанные решения; осуществлять эффективный поиск информации и критику источников; получать, обрабатывать и сохранять источники информации; формулировать и аргументировано отстаивать собственную позицию по различным проблемам истории. ОПК-16.3. Владеет представлениями о событиях российской и всемирной истории, основанными на принципе историзма; навыками анализа исторических источников; приёмами ведения дискуссии и полемики.
ОПК-7.1. Способен использовать программные и программно-аппаратные средства для моделирования и испытания систем защиты информационных систем.	ОПК-7.1.1. Знает подходы к моделированию и испытанию систем защиты информации информационных систем. ОПК-7.1.2. Умеет использовать программные и программно-аппаратные средства для моделирования систем защиты информационных систем. ОПК-7.1.3. Владеет навыками использования программных и программно-аппаратных средства для моделирования и испытания систем защиты информационных систем.
ОПК-7.2. Способен разрабатывать методики и тесты для анализа степени защищенности информационной системы и ее соответствия нормативным требованиям по защите информации.	ОПК-7.2.1. Знает нормативные требования по защите информации информационных систем. ОПК-7.2.2. Умеет разрабатывать методики для анализа защищенности информационных систем. ОПК-7.2.3. Владеет навыками разработки методики и тестов для анализа степени защищенности информационной системы и ее соответствия нормативным требованиям по защите информации.
ОПК-7.3. Способен проводить анализ защищенности и верификацию программного обеспечения информационных систем.	ОПК-7.3.1. Знает методы анализа защищенности и верификации программного обеспечения. ОПК-7.3.2. Умеет проводить анализ защищенности и верификацию программного обеспечения. ОПК-7.3.3. Владеет навыками анализа защищенности и верификации программного обеспечения информационных систем.

Выбор одной или нескольких обобщенных трудовых функций (полностью или частично), соответствующих профессиональной деятельности выпускников, приведена в приложении 1.

ОПОП устанавливает профессиональные компетенции, сформированные на основе профессиональных стандартов «Специалист по безопасности компьютерных систем и сетей», «Специалист по защите информации в автоматизированных системах», «Специалист по технической защите информации», в соответствии с которым выпускник должен овладеть комплексом трудовых функций (таблица 4).

Таблица 4. Профессиональные компетенции выпускников и индикаторы их достижения

Задача профессиональной деятельности	*Объект или область знания*	*Код и наименование профессиональной компетенции*	*Код и наименование индикатора достижения профессиональной компетенции*
Профессиональный стандарт «Специалист по безопасности компьютерных систем и сетей»			
Тип задач профессиональной деятельности – эксплуатационный			
реализация информационных технологий в сфере профессиональной деятельности с использованием защищенных автоматизированных систем; мониторинг информационной безопасности автоматизированных систем; управление информационной безопасностью автоматизированных систем; обеспечение восстановления работоспособности систем защиты информации при возникновении нештатных ситуаций.	информационные технологии, формирующие информационную инфраструктуру в условиях существования угроз в информационной сфере и задействующие информационно-технологические ресурсы, подлежащие защите; технологии обеспечения информационной безопасности автоматизированных систем.	ПК-1. Обеспечение информационной безопасности компьютерных систем и сетей	ПК-1.1. Знает основные подходы к обеспечению информационной безопасности компьютерных систем и сетей. ПК-1.2. Умеет настраивать компьютерные системы и сети в соответствии с требованиями по обеспечению информационной безопасности. ПК-1.3. Владеет навыками обеспечения информационной безопасности компьютерных систем и сетей.
Профессиональный стандарт «Специалист по защите информации в автоматизированных системах»			
Тип задач профессиональной деятельности – проектный			
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	автоматизированные системы, функционирующие в условиях существования угроз в информационной сфере и обладающие информационно-технологическими ресурсами, подлежащими защите; системы управления информационной безопасностью автоматизированных систем.	ПК-2. Разработка систем защиты информации автоматизированных систем.	ПК-2.1. Знает основные требования нормативных документов в области защиты информации в автоматизированных системах; знает основные подходы к разработке систем защиты информации автоматизированных систем. ПК-2.2. Умеет разрабатывать проекты систем защиты информации автоматизированных систем. ПК-2.3. Владеет навыками разработки систем защиты информации автоматизированных систем.

информационно-технологических ресурсов автоматизированных систем; выполнение проектов по созданию программ, комплексов программ, программно-аппаратных средств, баз данных, компьютерных сетей для защищенных автоматизированных систем; разработка систем управления информационной безопасностью автоматизированных систем.			
Тип задач профессиональной деятельности – научно-исследовательский			
сбор, обработка, анализ и систематизация научно-технической информации по проблематике информационной безопасности автоматизированных систем; подготовка научно-технических отчетов, обзоров, докладов, публикаций по результатам выполненных исследований; моделирование и исследование свойств защищенных автоматизированных систем, разработка модели угроз и модели нарушителя информационной безопасности, методик и тестов для анализа степени защищенности информационной системы и ее соответствия нормативным требованиям по защите информации; анализ защищенности	автоматизированные системы, функционирующие в условиях существования угроз в информационной сфере и обладающие информационно-технологическими ресурсами, подлежащими защите; информационные технологии, формирующие информационную инфраструктуру в условиях существования угроз в информационной сфере и задействующие информационно-технологические ресурсы, подлежащие защите; технологии обеспечения информационной безопасности автоматизированных систем.	ПК-3. Формирование требований к защите информации в автоматизированных системах.	ПК-3.1. Знает требования законодательства к защите информации в автоматизированных системах; знает подходы к формированию требований по защите информации в автоматизированных системах. ПК-3.2. Умеет формировать требования к защите информации в автоматизированных системах на основании нормативных документов. ПК-3.3. Владеет навыками формирования требований к защите информации в автоматизированных системах на основании анализа и моделирования системы защиты информации.

информации в автоматизированных системах и безопасности реализуемых информационных технологий; разработка эффективных решений по обеспечению информационной безопасности автоматизированных систем.			
Профессиональный стандарт «Специалист по технической защите информации»			
Тип задач профессиональной деятельности – организационно-управленческий			
организация работы коллектива, принятие управленческих решений в условиях спектра мнений, определение порядка выполнения работ; организационно-методическое обеспечение информационной безопасности автоматизированных систем; организация работ по созданию, внедрению, эксплуатации и сопровождению защищенных автоматизированных систем; контроль реализации политики информационной безопасности.	автоматизированные системы, функционирующие в условиях существования угроз в информационной сфере и обладающие информационно-технологическими ресурсами, подлежащими защите; системы управления информационной безопасностью автоматизированных систем.	ПК-4. Организация и проведение работ по технической защите информации.	ПК-4.1. Знает основы организации работы коллектива и методы принятия управленческих решений. ПК-4.2. Умеет применять методы принятия управленческих решения для организации работы коллектива в профессиональной деятельности. ПК-4.3. Владеет навыками организации и проведения работ по технической защите информации для обеспечения информационной безопасности автоматизированных систем.
Тип задач профессиональной деятельности – контрольно-аналитический			
контроль работоспособности и эффективности применяемых средств защиты информации; выполнение экспериментально-исследовательских работ при сертификации средств защиты информации и аттестации автоматизированных систем;	автоматизированные системы, функционирующие в условиях существования угроз в информационной сфере и обладающие информационно-технологическими ресурсами, подлежащими защите.	ПК-5. Проведение аттестации объектов на соответствие требованиям по защите информации.	ПК-5.1. Знает положения нормативных документов по аттестации объектов информатизации. ПК-5.2. Умеет проводить контроль защищенности автоматизированной системы от утечки по техническим каналам и от НСД к информации. ПК-5.3. Владеет навыками проведения аттестации автоматизированных систем на соответствие требованиям по защите информации.

проведение инструментального мониторинга защищенности автоматизированных систем и анализа его результатов.			

4. Структура образовательной программы

4.1. Структура ОПОП включает следующие блоки:

Блок 1 – Дисциплины (модули)

Блок 2 – Практика

Блок 3 – Государственная итоговая аттестация.

Таблица 5. Структура и объем ОПОП

Структура ОПОП		*Объем ОПОП и ее блоков в з.е.*
Блок 1	Дисциплины (модули)	не менее 282
Блок 2	Практика	не менее 27
Блок 3	Государственная итоговая аттестация	6 – 9
Объем ОПОП		330

4.2. В блоке 2 «Практика» реализуются следующие типы практик:

– типы учебной практики:

учебно-лабораторный практикум.

– типы производственной практики:

эксплуатационная практика;

научно-исследовательская работа;

преддипломная практика.

4.3. В Блок 3 «Государственная итоговая аттестация» входят:

подготовка к сдаче и сдача государственного экзамена;

подготовка к процедуре защиты и защита выпускной квалификационной работы.

4.4. ОПОП обеспечивает возможность обучающимся освоить элективные дисциплины (модули) и факультативные дисциплины (модули). Факультативные дисциплины (модули) не включаются в объем ОПОП.

4.5. В ОПОП выделяются обязательная часть и часть, формируемая участниками образовательных отношений.

К обязательной части ОПОП относятся дисциплины (модули) и практики, обеспечивающие формирование общепрофессиональных и профессиональных компетенций. Дисциплины (модули) и практики, обеспечивающие формирование

универсальных компетенций, включаются в обязательную часть ОПОП и в часть, формируемую участниками образовательных отношений.

5. Условия реализации образовательной программы

5.1. Условия реализации ОПОП формируются в соответствии с требованиями ФГОС ВО и включают в себя общесистемные требования, требования к материально-техническому и учебно-методическому обеспечению, требования к кадровым и финансовым условиям реализации ОПОП, а также требования к применяемым механизмам оценки качества образовательной деятельности и подготовки обучающихся по ОПОП.

5.2. Общесистемные требования к реализации ОПОП

5.2.1. Университет располагает на праве собственности или ином законном основании материально-техническим обеспечением образовательной деятельности (помещениями и оборудованием) для реализации ОПОП по Блоку 1 «Дисциплины (модули)» и Блоку 3 «Государственная итоговая аттестация» в соответствии с учебным планом.

5.2.2. Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к электронной информационно-образовательной среде университета из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети «Интернет», как на территории университета, так и вне ее.

Электронная информационно-образовательная среда университета обеспечивает:

– доступ к учебным планам, рабочим программам дисциплин (модулей), практик, электронным учебным изданиям и электронным образовательным ресурсам, указанным в рабочих программах дисциплин (модулей), практик;

– формирование электронного портфолио обучающегося, в том числе сохранение его работ и оценок за эти работы.

Функционирование электронной информационно-образовательной среды обеспечивается соответствующими средствами информационно-коммуникационных технологий и квалификацией работников, ее использующих и поддерживающих. Функционирование электронной информационно-образовательной среды соответствует законодательству Российской Федерации.

5.3. Требования к материально-техническому и учебно-методическому обеспечению ОПОП.

5.3.1. Помещения представляют собой учебные аудитории для проведения учебных занятий, предусмотренных ОПОП, оснащены оборудованием и техническими средствами обучения, состав которых определяется в рабочих программах дисциплин (модулей).

Минимально необходимый для реализации программы специалитета перечень материально-технического обеспечения включает в себя специально оборудованные помещения для проведения учебных занятий, в том числе:

лаборатории в области:

- физики, оснащенную учебно-лабораторными стендами по механике, электричеству и магнетизму, оптике;

- электроники и схемотехники, оснащенную учебно-лабораторными стендами для изучения работы компонентов узлов и блоков вычислительных устройств, рабочих мест разработчиков систем и устройств в системах автоматизированного проектирования, средствами для измерения и визуализации частотных и временных характеристик сигналов, средствами для измерения параметров электрических цепей, средствами генерирования сигналов;

- сетей и систем передачи информации, оснащенную рабочими местами на базе вычислительной техники, стендами сетей передачи информации с коммутацией пакетов и коммутацией каналов;

- безопасности вычислительных сетей, оснащенную стендами для изучения проводных и беспроводных компьютерных сетей, включающих абонентские устройства, коммутаторы, маршрутизаторы, точки доступа, межсетевые экраны, средства обнаружения компьютерных атак, системы углубленной проверки сетевых пакетов и системы защиты от утечки данных, анализаторы кабельных сетей;

- технической защиты информации, оснащенную специализированным оборудованием по защите информации от утечки по техническим каналам, техническими средствами контроля эффективности защиты информации от утечки по техническим каналам;

- программно-аппаратных средств защиты информации, оснащенную антивирусными программными комплексами, аппаратными средствами аутентификации пользователя, средствами анализа защищенности компьютерных сетей, устройствами чтения смарт-карт и радиометок, программно-аппаратными комплексами защиты информации, включающими в том числе средства криптографической защиты информации;

- автоматизированных систем в защищенном исполнении, оснащенную аппаратно-программными средствами управления доступом к данным, средствами криптографической защиты информации, средствами дублирования и восстановления данных, средствами мониторинга состояния автоматизированных систем, средствами контроля и управления доступом в помещения;

специально оборудованные кабинеты (классы, аудитории):

- информационных технологий, оснащенный рабочими местами на базе вычислительной техники и абонентскими устройствами, подключенными к сети "Интернет" с использованием проводных и/или беспроводных технологий;

- научно-исследовательской работы обучающихся, курсового и дипломного проектирования, оснащенный рабочими местами на базе вычислительной техники с набором необходимых для проведения и оформления результатов исследований дополнительных аппаратных и (или) программных средств, а также комплектом оборудования для печати;

- аудиторию (защищаемое помещение) для проведения учебных занятий, в ходе которых до обучающихся доводится информация ограниченного доступа, не содержащая сведений, составляющих государственную тайну;

- специальную библиотеку (библиотеку литературы ограниченного доступа), предназначенную для хранения и обеспечения использования в образовательном процессе нормативных и методических документов ограниченного доступа;

Компьютерные (специализированные) классы и лаборатории, если в них предусмотрены рабочие места на базе вычислительной техники, должны быть оборудованы современной вычислительной техникой из расчета одно рабочее место на каждого обучающегося при проведении занятий в данных классах (лабораториях).

Университет имеет лаборатории и (или) специально оборудованные кабинеты (классы, аудитории), обеспечивающие практическую подготовку выпускников в соответствии со специализацией программы специалитета.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Допускается частичная замена оборудования его виртуальными аналогами.

5.3.2. Университет обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения и сертифицированными средствами защиты информации, в том числе отечественного производства (состав

определяется в рабочих программах дисциплин (модулей) и подлежит обновлению при необходимости).

5.3.3. Использование в образовательном процессе печатных изданий обеспечено укомплектованностью библиотечного фонда из расчета не менее 0,25 экземпляра каждого из изданий, указанных в рабочих программах дисциплин (модулей), программах практик, на одного обучающегося из числа лиц, одновременно осваивающих соответствующую дисциплину (модуль), проходящих соответствующую практику.

5.3.4. Обучающимся обеспечен доступ (удаленный доступ) к современным профессиональным базам данных и информационным справочным системам, состав которых определяется в рабочих программах дисциплин (модулей).

5.3.5. Обучающиеся из числа инвалидов и лиц с ОВЗ обеспечены печатными и (или) электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

5.4. Требования к кадровым условиям реализации ОПОП.

5.4.1. Реализация ОПОП обеспечивается педагогическими работниками университета, а также лицами, привлекаемыми к реализации ОПОП на иных условиях.

5.4.2. Квалификация педагогических работников университета соответствует квалификационным требованиям, указанным в квалификационных справочниках, и (или) профессиональных стандартах.

5.4.3. Не менее 70 процентов численности педагогических работников университета и лиц, привлекаемых к реализации ОПОП на иных условиях, участвующих в реализации ОПОП (исходя из количества замещаемых ставок, приведенного к целочисленным значениям), ведут научную, учебно-методическую и (или) практическую работу, соответствующую профилю преподаваемой дисциплины (модуля).

5.4.4. Не менее 3 процентов численности педагогических работников университета, участвующих в реализации ОПОП, и лиц, привлекаемых к реализации ОПОП на иных условиях, (исходя из количества замещаемых ставок, приведенного к целочисленным значениям), являются руководителями и (или) работниками иных организаций, осуществляющими трудовую деятельность в профессиональной сфере, соответствующей профессиональной деятельности, к которой готовятся выпускники (имеют стаж работы в данной профессиональной сфере не менее 3 лет).

5.4.5. Доля педагогических работников университета (исходя из количества замещаемых ставок, приведенного к целочисленным значениям) составляет не менее 65 процентов от общего количества лиц, привлекаемых к реализации ОПОП.

5.4.6. Не менее 55 процентов численности педагогических работников университета и лиц, привлекаемых к образовательной деятельности университета на иных условиях, имеют ученую степень (в том числе ученую степень, полученную в иностранном государстве и признаваемую в Российской Федерации) и (или) ученое звание (в том числе ученое звание, полученное в иностранном государстве и признаваемое в Российской Федерации).

В реализации ОПОП принимает участие минимум один педагогический работник Организации, имеющий ученую степень или ученое звание по научной специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность» или по научной специальности, соответствующей направлениям подготовки кадров высшей квалификации по программам подготовки научно-педагогических кадров в адъюнктуре, входящим в укрупненную группу специальностей и направлений подготовки 10.00.00 «Информационная безопасность».

5.5. Требования к финансовым условиям реализации ОПОП.

5.5.1. Финансовое обеспечение реализации ОПОП осуществляется в объеме не ниже значений базовых нормативов затрат на оказание государственных услуг по реализации образовательных программ высшего образования – программ бакалавриата (магистратуры, специалитета) и значений корректирующих коэффициентов к базовым нормативам затрат, определяемых Минобрнауки России.

5.6. Требования к применяемым механизмам оценки качества образовательной деятельности и подготовки обучающихся по ОПОП.

5.6.1. Качество образовательной деятельности и подготовки обучающихся по ОПОП определяется в рамках системы внутренней оценки, а также системы внешней оценки, в которой университет принимает участие на добровольной основе.

5.6.2. В целях совершенствования ОПОП университет при проведении регулярной внутренней оценки качества образовательной деятельности и подготовки обучающихся по ОПОП привлекает работодателей и (или) их объединения, иных юридических и (или) физических лиц, включая педагогических работников университета.

В рамках внутренней системы оценки качества образовательной деятельности по ОПОП обучающимся предоставляется возможность оценивания условий, содержания, организации и качества образовательного процесса в целом и отдельных дисциплин (модулей) и практик.

5.6.3. Внешняя оценка качества образовательной деятельности по ОПОП в рамках процедуры государственной аккредитации осуществляется с целью подтверждения соответствия образовательной деятельности по ОПОП требованиям ФГОС ВО.

5.7. ОПОП, содержащая сведения, составляющие государственную тайну, разрабатывается и реализуется с соблюдением требований, предусмотренных законодательством Российской Федерации и иными нормативными правовыми актами в области защиты государственной тайны.

6. Особенности организации образовательного процесса для инвалидов и лиц с ограниченными возможностями здоровья

6.1. Для обучающихся инвалидов и лиц с ограниченными возможностями здоровья создаются условия организации образовательного процесса с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

6.2. При необходимости для обучающихся инвалидов и лиц с ограниченными возможностями здоровья на основе настоящей ОПОП и в соответствии с локальными нормативными актами университета разрабатывается адаптированная ОПОП. Для инвалидов адаптированная программа формируется в соответствии с индивидуальной программой реабилитации инвалида.

Приложение 1

Выбор обобщенных трудовых функций, соответствующих профессиональной деятельности выпускников

Наименование профессионального стандарта			**Наименование образовательной программы**		
«Специалист по безопасности компьютерных систем и сетей»			**10.05.03 Информационная безопасность автоматизированных систем, специализация N 7 «Анализ безопасности информационных систем»**		
ОТФ:	**ТФ:**	**ТД:**	**Типы задач профессиональной деятельности**	**Задачи профессиональной деятельности**	**Код и наименование профессиональной компетенции**
Оценивание уровня безопасности компьютерных систем и сетей	Проведение контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации в компьютерных системах и сетях	Оценка работоспособности применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик Оценка эффективности применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик Определение уровня защищенности и доверия программно-аппаратных средств защиты информации	эксплуатационный	реализация информационных технологий в сфере профессиональной деятельности с использованием защищенных автоматизированных систем;	ПК-1. Обеспечение информационной безопасности компьютерных систем и сетей

	Проведение анализа безопасности компьютерных систем	Определение уровня защищенности и доверия в компьютерных системах Оценка рисков, связанных с осуществлением угроз безопасности в отношении компьютерных систем Оценка соответствия механизмов безопасности компьютерной системы требованиям существующих нормативных документов, а также их адекватности существующим рискам Подготовка аналитического отчета по результатам проведенного анализа уровня защищенности и доверия в компьютерных системах Формулирование предложений по устранению выявленных уязвимостей компьютерных сетей		мониторинг информационной безопасности автоматизированных систем;	

	Разработка требований по защите, формирование политик безопасности компьютерных систем и сетей	Формирование политик безопасности компьютерных систем Консультирование по вопросам безопасности компьютерных систем Разработка профилей защиты и заданий по безопасности Разработка технических заданий на создание средств защиты информации Принятие решения о необходимости защиты информации, содержащейся в информационной системе Классификация информационной системы по требованиям защиты информации Определение угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в компьютерной системе и сети Разработка модели угроз безопасности информации Задание требований к защите информации компьютерной системы Разработка руководящих документов по защите информации в организации		управление информационной безопасностью автоматизированных систем;	

	Проведение экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов в компьютерных системах и сетях	Определение свойств аппаратных средств в составе компьютерной системы и их фактического и первоначального состояния Определение характеристик операционной системы и используемых технологий системного программирования в компьютерных системах и сетях Анализ функциональных свойств программного обеспечения в компьютерных системах и сетях Определение причин и условий изменения свойств исследуемой информации в компьютерных системах и сетях Выработка предложений по устранению выявленных уязвимостей в компьютерных системах и сетях		обеспечение восстановления работоспособности систем защиты информации при возникновении нештатных ситуаций.	
Наименование профессионального стандарта			**Наименование образовательной программы**		
«Специалист по защите информации в автоматизированных системах»			**10.05.03 Информационная безопасность автоматизированных систем, специализация N 7 «Анализ безопасности информационных систем»**		
ОТФ:	**ТФ:**	**ТД:**	**Типы задач профессиональной деятельности**	**Задачи профессиональной деятельности**	**Код и наименование профессиональной компетенции**
Разработка систем защиты информации автоматизированных систем, используемых в том числе на объектах критической информационной	Тестирование систем защиты информации автоматизированных систем	Проведение анализа структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем	проектный	сбор и анализ исходных данных для проектирования защищенных автоматизированных систем;	ПК-2. Разработка систем защиты информации автоматизированных систем.

инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости		Выявление уязвимости информационно-технологических ресурсов автоматизированных систем Выявление основных угроз безопасности информации в автоматизированных системах			
	Разработка эксплуатационной документации на системы защиты информации автоматизированных систем	Анализ технической документации информационной инфраструктуры автоматизированной системы Анализ защищенности информационной инфраструктуры автоматизированной системы Формирование требований по защите информации, включая использование математического аппарата для решения прикладных задач Документирование программного обеспечения, технических средств, баз данных и компьютерных сетей с учетом требований по обеспечению защиты информации Анализ структурных и функциональных схем защищенных автоматизированных информационных систем Обоснование критериев эффективности функционирования защищенных автоматизированных информационных систем Использование программно-		разработка политик информационной безопасности автоматизированных систем;	

		аппаратных средств обеспечения безопасности информации в автоматизированных системах			
	Разработка проектных решений по защите информации в автоматизированных системах	Разработка модели угроз безопасности информации и модели нарушителя в автоматизированных системах Разработка моделей автоматизированных систем и подсистем безопасности автоматизированных систем Разработка проектов нормативных документов, регламентирующих работу по защите информации		разработка защищенных автоматизированных систем в сфере профессиональной деятельности, обоснование выбора способов и средств защиты информационно-технологических ресурсов автоматизированных систем;	
	Разработка программных и программно-аппаратных средств для систем защиты информации автоматизированных систем	Разработка технической документации на компоненты автоматизированных систем в соответствии с требованиями Единой системы конструкторской документации и Единой системы программной документации Синтез структурных и функциональных схем защищенных автоматизированных систем Разработка программного обеспечения, технических средств, баз данных и компьютерных сетей с учетом требований по обеспечению защиты информации Разработка электронных схем с учетом требований по защите информации Оптимизация работы электронных		выполнение проектов по созданию программ, комплексов программ, программно-аппаратных средств, баз данных, компьютерных сетей для защищенных автоматизированных систем;	

		схем с учетом требований по защите информации			
	Разработка проектных решений по защите информации в автоматизированных системах	Разработка предложений по совершенствованию системы управления безопасностью информации в автоматизированных системах		разработка систем управления информационной безопасностью автоматизированных систем.	
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	Обоснование необходимости защиты информации в автоматизированной системе	Анализ характера обрабатываемой информации и определение перечня информации, подлежащей защите Выявление степени участия персонала в обработке защищаемой информации Планирование мероприятий по обеспечению защиты информации в автоматизированной системе Определение требуемого класса (уровня) защищенности автоматизированной системы Обоснование необходимости использования криптографических средств защиты информации	научно-исследовательский	сбор, обработка, анализ и систематизация научно-технической информации по проблематике информационной безопасности автоматизированных систем;	ПК-3. Формирование требований к защите информации в автоматизированных системах.
		Разработка отчетных документов и разделов технических заданий		подготовка научно-технических отчетов, обзоров, докладов, публикаций по результатам выполненных исследований;	
	Моделирование защищенных автоматизированных систем с целью анализа их	Разработка аналитических и компьютерных моделей автоматизированных систем и подсистем безопасности автоматизированных систем		моделирование и исследование свойств защищенных автоматизированных систем, разработка	

	уязвимостей и эффективности средств и способов защиты информации	Исследование аналитических и компьютерных моделей автоматизированных систем и подсистем безопасности автоматизированных систем Разработка модели угроз безопасности информации и нарушителей в автоматизированных системах Исследование программных, архитектурно-технических и схемотехнических решений компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах Анализ информационной инфраструктуры и безопасности информации автоматизированных систем Разработка предложений по совершенствованию системы управления информационной безопасностью автоматизированных систем		модели угроз и модели нарушителя информационной безопасности, методик и тестов для анализа степени защищенности информационной системы и ее соответствия нормативным требованиям по защите информации;	
	Определение угроз безопасности информации, обрабатываемой автоматизированной системой	Формирование разделов технических заданий на создание систем защиты информации автоматизированных систем Разработка систем защиты информации автоматизированных систем с учетом действующих		анализ защищенности информации в автоматизированных системах и безопасности реализуемых информационных технологий;	

		нормативно-правовых документов Определение комплекса мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации автоматизированных систем Определение оценки возможностей внешних и внутренних нарушителей Разработка модели угроз безопасности информации автоматизированной системы Обоснование перечня сертифицированных средств защиты информации, необходимых для создания системы защиты информации автоматизированной системы Анализ требований к назначению, структуре и конфигурации создаваемой автоматизированной системы с целью выявления угроз безопасности информации Определение структурно-функциональных характеристик информационной системы в соответствии с требованиями нормативных правовых документов в области защиты информации			
	Разработка архитектуры системы защиты информации	Проведение оценки показателей качества и эффективности работы вычислительных систем, программных и программно-		разработка эффективных решений по обеспечению информационной безопасности	

	автоматизированной системы	аппаратных средств, используемых для построения систем защиты информации Проведение технико-экономической оценки целесообразности создания системы защиты информации автоматизированной системы Определение порядка обработки информации в автоматизированной системе Формирование разделов технических заданий на создание систем защиты информации автоматизированных систем Разработка проектной документации на системы защиты автоматизированных систем Оформление заявки на разработку системы защиты информации автоматизированной системы		автоматизированных систем.	
Наименование профессионального стандарта			**Наименование образовательной программы**		
«Специалист по технической защите информации»			**10.05.03 Информационная безопасность автоматизированных систем, специализация N 7 «Анализ безопасности информационных систем»**		
ОТФ:	**ТФ:**	**ТД:**	**Типы задач профессиональной деятельности**	**Задачи профессиональной деятельности**	**Код и наименование профессиональной компетенции**
Организация и проведение работ по технической защите информации	Сопровождение системы защиты информации в ходе ее эксплуатации	Организация контроля состояния системы защиты информации Руководство разработкой предложений по совершенствованию организационных и технических мероприятий по технической защите	организационно-управленческий	организация работы коллектива, принятие управленческих решений в условиях спектра мнений, определение порядка выполнения работ;	ПК-4. Организация и проведение работ по технической защите информации.

		информации и оценке их эффективности, совершенствованию системы технической защиты информации в организации Организация работ по участию сотрудников подразделения в расследовании нарушений требований и норм технической защиты информации в организации и разработка предложений по предупреждению нарушений Организация выполнения работ по техническому обслуживанию технических и программно-технических средств защиты информации Организация выполнения работ по устранению неисправностей и ремонту технических, программных (программно-технических) средств защиты информации, входящих в состав системы защиты информации организации Организация мероприятий по выводу из эксплуатации систем информатизации и утилизации их элементов			
	Аналитическое обоснование необходимости создания системы защиты информации в организации	Определение перечня информации (сведений) ограниченного доступа, подлежащих защите в организации Определение перечня объектов информатизации, на которых производится обработка информации ограниченного доступа		организационно-методическое обеспечение информационной безопасности автоматизированных систем;	

		Анализ данных о назначении, функциях, условиях функционирования технических средств обработки информации ограниченного доступа, установленных на объектах информатизации, и характере обрабатываемой на них информации Определение перечня выделенных (защищаемых) помещений, в которых происходит обсуждение сведений ограниченного доступа Анализ сведений, обсуждаемых в выделенных (защищаемых) помещениях Предпроектное обследование объектов вычислительной техники и выделенных (защищаемых) помещений Организация проведения научных исследований по вопросам технической защиты информации, выполняемых в организации Разработка модели угроз безопасности информации в организации Разработка аналитического обоснования необходимости создания системы защиты информации в организации Разработка технического задания на			

		создание системы защиты информации			
	Ввод в эксплуатацию системы защиты информации в организации	Организация проведения специальных исследований и специальных проверок технических средств обработки информации ограниченного доступа Организация установки и настройки технических, программных (программно-технических) средств защиты информации, входящих в состав системы защиты информации организации, в соответствии с техническим проектом и инструкциями по эксплуатации Разработка организационно-распорядительных документов, определяющих мероприятия по защите информации в организации Разработка и реализация организационных мер, обеспечивающих эффективность системы защиты информации Организация проведения инструктажа руководящего состава и обучения персонала по вопросам технической защиты информации Организация опытной эксплуатации и доработки системы защиты информации Разработка программы и методики предварительных испытаний системы защиты информации		организация работ по созданию, внедрению, эксплуатации и сопровождению защищенных автоматизированных систем;	

		Организация приемочных испытаний системы защиты информации Подготовка объектов вычислительной техники и выделенных (защищаемых) помещений к аттестации по требованиям безопасности информации Организация и сопровождение аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации Ввод системы защиты информации в эксплуатацию			
	Сопровождение системы защиты информации в ходе ее эксплуатации	Организация контроля состояния системы защиты информации Организация работ по участию сотрудников подразделения в расследовании нарушений требований и норм технической защиты информации в организации и разработка предложений по предупреждению нарушений		контроль реализации политики информационной безопасности.	
Проведение аттестации объектов на соответствие требованиям по защите информации	Проведение аттестации объектов вычислительной техники на соответствие требованиям по защите информации	Разработка программы и методик аттестационных испытаний объектов вычислительной техники на соответствие требованиям по защите информации	контрольно-аналитический	контроль работоспособности и эффективности применяемых средств защиты информации;	ПК-5. Проведение аттестации объектов на соответствие требованиям по защите информации.
		Проведение аттестационных испытаний объектов вычислительной техники на		выполнение экспериментально-исследовательских работ	

		соответствие требованиям по защите информации		при сертификации средств защиты информации и аттестации автоматизированных систем;	
		Подготовка заключения по результатам аттестации объектов вычислительной техники на соответствие требованиям по защите информации Подготовка аттестата соответствия объектов вычислительной техники требованиям по защите информации		проведение инструментального мониторинга защищенности автоматизированных систем и анализа его результатов.	