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 «31» марта 2021 г. № 1/8(550)

ОСНОВНАЯ ПРОФЕССИОНАЛЬНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА ВЫСШЕГО ОБРАЗОВАНИЯ

по направлению подготовки

10.03.01 Информационная безопасность

Направленность (профиль) программы –

Техническая защита информации

Присваиваемая квалификация – бакалавр

Сыктывкар
2021

Китайгородский Михаил Дмитриевич

Подписано цифровой подписью: Китайгородский Михаил Дмитриевич
Дата: 2024.07.01 13:13:43 +03'00'

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 направлению подготовки 10.03.01 Информационная безопасность (далее – ФГОС ВО) (утв. приказом Минобрнауки России от 17.11.2020 № 1427), с учетом профессиональных стандартов «Специалист по защите информации в автоматизированных системах» (утв. приказом Минтруда России от 15.09.2016 № 522н) (действует до 28.02.2023), «Специалист по защите информации в автоматизированных системах» (утв. Приказом Минтруда России от 14.09.2022 N 525н) (действует с 01.03.2023), «Специалист по технической защите информации» (утв. приказом Минтруда России от 01.11.2016 № 599н) (действует до 28.02.2023), Специалист по технической защите информации (утв. Приказом Минтруда России от 09.08.2022 N 474н) (действует с 01.03.2023).

1.2. Обучение по ОПОП может осуществляться в очной и очно-заочной формах обучения.

1.3. Сроки обучения:

– в очной форме обучения, включая каникулы, предоставляемые после прохождения государственной итоговой аттестации, составляет 4 года;

– в очно-заочной форме обучения увеличивается не менее чем на 6 месяцев и не более чем на 1 год по сравнению со сроком получения образования в очной форме обучения;

– 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 240 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 10.03.01 Информационная безопасность, локальными актами университета, а также учебным планом в части контактной работы при проведении учебных занятий.

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

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 техники и технологии, охватывающей совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере).

2.2. Типы задач профессиональной деятельности выпускника по ОПОП:

– эксплуатационный;

– экспериментально-исследовательский;

– организационно-управленческий.

2.3. Перечень основных задач профессиональной деятельности выпускников.

Основные задачи профессиональной деятельности определяются требованиями ФГОС ВО по направлению подготовки 10.03.01 Информационная безопасность, профилем (направленностью) ОПОП – Техническая защита информации и требованиями профессиональных

стандартов «Специалист по защите информации в автоматизированных системах» и «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)*
06 Связь, информационные и коммуникационные технологии	эксплуатационный	Установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований. Администрирование подсистем информационной безопасности объекта. Участие в проведении аттестации объектов информатизации по требованиям безопасности информации и аудите информационной безопасности автоматизированных систем.	Объекты информатизации, включая компьютерные, автоматизированные, телекоммуникационные, информационные и информационно-аналитические системы, информационные ресурсы и информационные технологии в условиях существования угроз в информационной сфере (далее - объекты информатизации). Технологии обеспечения информационной безопасности объектов различного уровня (система, объект системы, компонент объекта), которые связаны с информационными технологиями, используемыми на этих объектах (далее -

			технологии обеспечения информационной безопасности).
	экспериментально-исследовательский	Сбор, изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования. Проведение экспериментов по заданной методике, обработка и анализ их результатов. Проведение вычислительных экспериментов с использованием стандартных программных средств.	Объекты информатизации.
	организационно-управленческий	Осуществление организационно-правового обеспечения информационной безопасности объекта защиты. Организация работы малых коллективов исполнителей. Участие в совершенствовании системы управления информационной безопасностью. Изучение и обобщение опыта работы других учреждений, организаций и предприятий в области защиты информации, в том числе информации ограниченного доступа. Контроль эффективности реализации политики	Объекты информатизации. Технологии обеспечения информационной безопасности. Процессы управления информационной безопасностью защищаемых объектов.

		информационной безопасности объекта защиты.	

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 поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.1. Знает принципы сбора, отбора и обобщения информации. УК-1.2. Умеет соотносить разнородные явления и систематизировать их в рамках избранных видов деятельности. УК-1.3. Способен грамотно, логично, аргументированно формировать собственные суждения и оценки
Разработка и реализация проектов	УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.1. Знает правовые нормы, необходимые для достижения поставленной цели при реализации проекта. УК-2.2. Умеет определять круг задач в рамках избранных видов профессиональной деятельности, планировать собственную деятельность, исходя из имеющихся ресурсов, соотносить главное и второстепенное, решать поставленные задачи в рамках избранных видов профессиональной деятельности. УК-2.3. Владеет навыками отбора оптимальных технологий целедостижения; навыками работы с нормативными

		документами.
Командная работа и лидерство	УК-3. Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде	УК-3.1. Знает различные приёмы и способы социализации личности и социального взаимодействия. УК-3.2. Умеет строить отношения с окружающими людьми, с коллегами. УК-3.3. Способен определять свою роль в команде на основе использования стратегии сотрудничества для достижения поставленной цели
Коммуникация	УК-4. Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(ых) языке(ах)	УК-4.1. Знает основы коммуникации, нормы, правила и особенности её осуществления в устной и письменной формах на русском и иностранном(ых) языке(ах). УК-4.2. Умеет применять правила и нормы деловой коммуникации на русском и иностранном(ых) языке(ах). УК-4.3. Владеет навыками применения коммуникативных технологий на русском и иностранном(ых) языке(ах) для академического и профессионального взаимодействия
Межкультурное взаимодействие	УК-5. Способен воспринимать межкультурное разнообразие общества в социально-историческом, этическом и философском контекстах	УК-5.1. Знает основные категории философии, законы исторического развития, основы межкультурной коммуникации. УК-5.2. Умеет анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия. УК-5.3. Владеет навыками коммуникации с представителями иных национальностей и конфессий с соблюдением этических и межкультурных норм
Самоорганизация и саморазвитие (в том числе здоровьесбережение)	УК-6. Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни	УК-6.1. Знает основные принципы самовоспитания и самообразования, профессионального и личностного развития, исходя из этапов карьерного роста и требований рынка труда. УК-6.2. Умеет планировать своё рабочее время и время для саморазвития, формулировать

		цели личностного и профессионального развития и условия их достижения, исходя из тенденций развития области профессиональной деятельности, индивидуально-личностных особенностей. УК-6.3. Способен выстраивать траекторию саморазвития посредством обучения по дополнительным образовательным программам.
	УК-7. Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности	УК-7.1. Знает основы здорового образа жизни, здоровьесберегающих 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	УК-10.1. Иметь представление о понятии и сущности экстремизма, терроризма, коррупции; формах их проявления в современном обществе; их общественной опасности; основы

	противодействовать им в профессиональной деятельности	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

Категория (группа) общепрофессио-нальных компетенций	*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 информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности	ОПК-2.1. Знает основные информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства и методы использования. ОПК-2.1. Умеет применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства. ОПК-2.1. Владеет навыками решения задач профессиональной деятельности с использованием информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства.
	ОПК-3. Способен использовать необходимые математические методы 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 применять необходимые физические законы и модели для решения задач профессиональной деятельности	ОПК-4.1. Знает физические законы и модели. ОПК-4.2. Умеет определять и применять необходимые физические законы и модели. 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 в сфере профессиональной деятельности	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 технической защите информации.
	ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа 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 использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности	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 осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности	ОПК-8.1. Знает основные методы поиска информации по ключевым словам; основные источники информации по вопросам обеспечения информационной безопасности. 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 по профилю своей деятельности. 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 применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ОПК-9.1. Знает современные средства криптографической и технической защиты информации. ОПК-9.2. Умеет использовать и настраивать современные средства криптографической и технической защиты информации. ОПК-9.3. Владеет навыками решения задач профессиональной деятельности с использованием современных средства криптографической и технической защиты информации.
	ОПК-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	ОПК-10.1. Знает принципы формирования политики информационной безопасности в информационных системах. ОПК-10.2. Умеет разрабатывать частные политики информационной безопасности информационных систем; определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных систем. ОПК-10.3. Владеет навыками реализации политики информационной безопасности объектов защиты; навыками применения комплексного подхода к обеспечению информационной безопасности объекта защиты.
	ОПК-11. Способен проводить эксперименты по заданной методике и обработку их результатов	ОПК-11.1. Знает основные методы экспериментальных исследований оценки защищенности объектов информатизации; основные понятия об измерениях и единицах физических величин; основные виды средств измерения и их классификацию; методы измерений. ОПК-11.2. Умеет проводить эксперименты по заданной методике, обрабатывать и оценивать погрешности измерений; проводить оценку достоверности экспериментальных результатов; классифицировать основные виды средств измерений; применять основные методы и

		принципы измерений; применять методы и средства обеспечения единства и точности измерений; применять аналоговые и цифровые измерительные приборы, измерительные генераторы; применять методические оценки защищенности информационных объектов. ОПК-11.3. Владеет навыками проведения физического эксперимента и обработки его результатов; методами расчета и инструментального контроля показателей технической защиты информации.
	ОПК-12. Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	ОПК-12.1. Знает основные методы управления информационной безопасностью; основные подходы к анализу исходных данных и проектированию системы защиты информации; основные методики оценки рисков и проведения технико-экономического обоснования. ОПК-12.2. Умеет оценивать информационные риски в информационных системах; проводить расчёты для технико-экономического обоснования проектных решений; разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных систем. ОПК-12.3. Владеет методами управления информационной безопасностью информационных систем; методами оценки информационных рисков.
	ОПК-13. Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма	ОПК-13.1. 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, выдающихся деятелей отечественной истории; различные оценки и периодизации

		Отечественной истории. ОПК-13.2. 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-13.3. Владеет представлениями о событиях российской и всемирной истории, основанными на принципе историзма; навыками анализа исторических источников; приёмами ведения дискуссии и полемики.
Направленность (профиль) Техническая защита информации	ОПК-3.1. Способен проводить работы по установке, настройке, испытаниям и техническому обслуживанию средств защиты информации от утечки по техническим каналам	ОПК-3.1.1. Знает классификацию и особенности применения технических средств защиты информации от утечки по техническим каналам. ОПК-3.1.2. Умеет устанавливать и настраивать технические средства защиты информации от утечки по техническим каналам. ОПК-3.1.3. Владеет навыками испытания и обслуживания технических средств защиты информации от утечки по техническим каналам.
	ОПК-3.2. Способен проводить работы по установке, настройке, испытаниям и техническому обслуживанию средств защиты информации от несанкционированного доступа	ОПК-3.2.1. Знает классификацию и особенности применения технических средств защиты информации от несанкционированного доступа и средства антивирусной защиты. ОПК-3.2.2. Умеет устанавливать и настраивать технические средства защиты информации от несанкционированного доступа и средства антивирусной защиты. ОПК-3.2.3. Владеет навыками испытания и обслуживания

		технических средств защиты информации от несанкционированного доступа и средства антивирусной защиты.
	ОПК-3.3. Способен проводить контроль эффективности защиты информации от утечки по техническим каналам	ОПК-3.3.1. Знает основные понятия в области аттестации объектов информатизации; - основные методы оценки защищенности объектов информатизации от утечки по техническим каналам. ОПК-3.3.2. Умеет проводить оценку защищенности объектов информатизации от утечки информации по техническим каналам. ОПК-3.3.3. Владеет навыками проведения специального обследования объектов информатизации и оценки защищенности объектов информатизации от утечки информации по техническим каналам.
	ОПК-3.4. Способен проводить контроль защищенности информации от несанкционированного доступа	ОПК-3.4.1. Знает основные понятия в области аттестации объектов информатизации; основные методы оценки защищенности объектов информатизации от несанкционированного доступа к информации. ОПК-3.4.2. Умеет проводить оценку защищенности объектов информатизации от несанкционированного доступа к информации. ОПК-3.4.3. Владеет навыками проведения оценки защищенности объектов информатизации от несанкционированного доступа к информации.

ОПОП устанавливает профессиональные компетенции, сформированные на основе профессиональных стандартов «Специалист по защите информации в автоматизированных системах» и «Специалист по технической защите информации», в соответствии с которыми 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*
Тип задач профессиональной деятельности - эксплуатационный			
Установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований. Администрирование подсистем информационной безопасности объекта. Участие в проведении аттестации объектов информатизации по требованиям безопасности информации и аудите информационной безопасности автоматизированных систем.	Объекты информатизации. Технологии обеспечения информационной безопасности.	ПК-1 Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации	ПК-1.1. Знает методы, средства и технологии обеспечения защиты информации в автоматизированных системах. ПК-1.2. Умеет применять методы, средства и технологии обеспечения защиты информации в автоматизированных системах. ПК-1.3. Владеет навыками обеспечения защиты информации в автоматизированных системах в процессе их эксплуатации.
Тип задач профессиональной деятельности - организационно-управленческий			
Осуществление организационно-правового обеспечения информационной безопасности	Объекты информатизации. Технологии обеспечения информационной	ПК-2 Внедрение систем защиты информации автоматизированных систем	ПК-2.1. Знает подходы к внедрению систем защиты информации в автоматизированных системах.

объекта защиты. Организация работы малых коллективов исполнителей. Участие в совершенствовании системы управления информационной безопасностью. Изучение и обобщение опыта работы других учреждений, организаций и предприятий в области защиты информации, в том числе информации ограниченного доступа. Контроль эффективности реализации политики информационной безопасности объекта защиты.	безопасности.		ПК-2.2. Умеет устанавливать и настраивать средства защиты информации. ПК-2.3. Владеет навыками внедрения систем защиты информации в автоматизированных системах.
Тип задач профессиональной деятельности - экспериментально-исследовательский			
Сбор, изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования. Проведение экспериментов по заданной методике, обработка и анализ их результатов. Проведение вычислительных экспериментов с	Объекты информатизации.	ПК-3 Проведение контроля защищенности информации	ПК-3.1. Знает методы и средства контроля защищенности информации от утечки по техническим каналам и от несанкционированного доступа; нормативные правовые акты и методические документы по контролю защищенности. ПК-3.2. Умеет проводить измерения по заданной

использованием стандартных программных средств.			методике. ПК-3.3. Владеет навыками проведения контроля защищенности информации; навыками оформления документации по результатам контроля.

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 201
Блок 2	Практика	не менее 18
Блок 3	Государственная итоговая аттестация	6-9
Объем ОПОП		240

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

– типы учебной практики:

учебно-лабораторная практика;

– типы производственной практики:

эксплуатационная практика;

преддипломная практика.

4.3. В Блок 3 «Государственная итоговая аттестация» входит – 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.

Объем обязательной части, без учета объема государственной итоговой аттестации, составляет 77,1 процентов общего объема ОПОП.

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).

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

Минимально необходимый для реализации программы бакалавриата перечень материально-технического обеспечения включает в себя

специально оборудованные помещения для проведения учебных занятий, в том числе:

лаборатории:

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

- электротехники, электроники и схемотехники, оснащенные учебно-лабораторными стендами и контрольно-измерительной аппаратурой для измерения частотных свойств, форм 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, структурированной кабельной системой, стойками с телекоммуникационным оборудованием, системой питания и вентиляции, эмулятором (эмуляторами) активного сетевого оборудования, специализированным программным обеспечением для настройки телекоммуникационного оборудования;

- технической защиты информации, оснащенную специализированным оборудованием по защите информации от утечки по акустическому каналу, каналу побочных электромагнитных излучений и наводок, акустовибрационному и акустоэлектрическому каналам (для направленности (профиля) Техническая защита информации), техническими средствами контроля эффективности защиты информации от утечки по указанным каналам;

- программно-аппаратных средств защиты информации, оснащенную антивирусными программными комплексами, аппаратными средствами аутентификации пользователя, программно-аппаратными комплексами защиты информации, включающими в том числе средства криптографической защиты информации (средствами анализа

защищенности компьютерных сетей, аппаратно-программными средствами управления доступом к данным, стендами для изучения проводных и беспроводных компьютерных сетей, включающими абонентские устройства, коммутаторы, маршрутизаторы, средства анализа сетевого трафика, межсетевые экраны);

специально оборудованные кабинеты (классы, аудитории):

- информатики, технологий и методов программирования, оснащенный рабочими местами на базе вычислительной техники, подключенными к локальной вычислительной сети и сети "Интернет", сетевым программным обеспечением, обучающим программным обеспечением;

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, оборудованы современной вычислительной техникой из расчета одно рабочее место на каждого обучаемого при проведении занятий в данных классах (лабораториях).

Университет имеет лаборатории и (или) специально оборудованные кабинеты (классы, аудитории), обеспечивающие практическую подготовку в соответствии с направленностью (профилем) программы бакалавриата.

Допускается частичная замена оборудования его виртуальными аналогами.

5.3.2. Университет обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства, требуемого для реализации ОПОП и указанного в рабочих программах дисциплин (модулей).

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. Не менее 50 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).

5.4.6. Доля педагогических работников университета (исходя из количества замещаемых ставок, приведенного к целочисленным значениям) составляет не менее 55 процентов от общего количества лиц, привлекаемых к реализации ОПОП.

5.4.7. В реализации ОПОП принимает участие минимум один педагогический работник университета, 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 ЗАЩИТЕ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ (утв. приказом Минтруда России от 15.09.2016 № 522н) (действует до 28.02.2023)			**10.03.01 Информационная безопасность, профиль «Техническая защита информации»**		
ОТФ:	**ТФ:**	**ТД:**	**Типы задач профессиональной деятельности**	**Задачи профессиональной деятельности**	**Код и наименование профессиональной компетенции**
Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации	Управление защитой информации в автоматизированных системах	Анализ воздействия изменений конфигурации автоматизированной системы на ее защищенность Составление комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе Оценка последствий от реализации угроз безопасности информации в автоматизированной системе Анализ изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации	эксплуатационный	Установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований.	ПК-1 обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации
	Обеспечение	Обнаружение неисправностей			

	работоспособности систем защиты информации при возникновении нештатных ситуаций	в работе системы защиты информации автоматизированной системы Устранение неисправностей в работе системы защиты информации автоматизированной системы Резервирование программного обеспечения, технических средств, каналов передачи данных автоматизированной системы управления на случай возникновения нештатных ситуаций Создание альтернативных мест хранения и обработки информации на случай возникновения нештатных ситуаций Восстановление после сбоев и отказов программного обеспечения автоматизированных систем			
	Администрирование систем защиты информации автоматизированных систем	Установка обновлений программного обеспечения автоматизированной системы Обеспечение безопасности информации с учетом требования эффективного функционирования автоматизированной системы Управление полномочиями		Администрирование подсистем информационной безопасности объекта.	

		пользователей автоматизированной системы Информирование пользователей о правилах эксплуатации автоматизированной системы с учетом требований по защите информации Проведение занятий с персоналом по работе с системой защиты информации автоматизированной системы, включая проведение практических занятий с персоналом на макетах или в тестовой зоне Внесение изменений в эксплуатационную документацию и организационно-распорядительные документы по системе защиты информации автоматизированной системы			
	Диагностика систем защиты информации автоматизированных систем	Обнаружение инцидентов в процессе эксплуатации автоматизированной системы Идентификация инцидентов в процессе эксплуатации автоматизированной системы Оценка защищенности автоматизированных систем с		Участие в проведении аттестации объектов информатизации по требованиям безопасности информации и аудите	

		помощью типовых программных средств Устранение инцидентов, возникших в процессе эксплуатации автоматизированной системы Расчет показателей эффективности защиты информации, обрабатываемой в автоматизированных системах Инструментальный контроль показателей эффективности защиты информации, обрабатываемой в автоматизированных системах		информационной безопасности автоматизированных систем.	
	Мониторинг защищенности информации в автоматизированных системах	Выработка рекомендаций для принятия решения о модернизации системы защиты информации автоматизированной системы Выработка рекомендаций для принятия решения о повторной аттестации автоматизированной системы или о проведении дополнительных аттестационных испытаний Выявление угроз безопасности информации в автоматизированных системах Принятие мер защиты			

		информации при выявлении новых угроз безопасности информации Анализ недостатков в функционировании системы защиты информации автоматизированной системы Устранение недостатков в функционировании системы защиты информации автоматизированной системы			
	Аудит защищенности информации в автоматизированных системах	Оценка информационных рисков Обоснование и контроль результатов управленческих решений в области безопасности информации автоматизированных систем Экспертиза состояния защищенности информации автоматизированных систем Обоснование критериев эффективности функционирования защищенных автоматизированных систем			
Внедрение систем защиты информации автоматизированных систем	Установка и настройка средств защиты информации в автоматизированных системах	Входной контроль качества комплектующих изделий системы защиты информации автоматизированной системы Осуществление автономной наладки технических и	эксплуатационный	Установка, настройка, эксплуатация и поддержание в работоспособном состоянии	ПК-1 обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации

		программных средств системы защиты информации автоматизированной системы Проведение приемочных испытаний системы защиты информации автоматизированной системы Внесение в эксплуатационную документацию изменений, направленных на устранение недостатков, выявленных в процессе испытаний		компонентов системы обеспечения информационной безопасности с учетом установленных требований.	
Внедрение систем защиты информации автоматизированных систем	Разработка организационно-распорядительных документов по защите информации в автоматизированных системах	Определение правил и процедур управления системой защиты информации автоматизированной системы Определение правил и процедур выявления инцидентов Определение правил и процедур мониторинга обеспечения уровня защищенности информации автоматизированной системы Определение правил и процедур защиты информации при выводе автоматизированной системы из эксплуатации Определение правил и процедур реагирования на инциденты	организационно-управленческий	Осуществление организационно-правового обеспечения информационной безопасности объекта защиты.	ПК-2 внедрение систем защиты информации автоматизированных систем

	Внедрение организационных мер по защите информации в автоматизированных системах	Проведение проверки полноты описания в организационно-распорядительных документах на автоматизированную систему действий персонала по реализации организационных мер защиты информации Проведение занятий с персоналом по работе с системой защиты информации автоматизированной системы, включая проведение практических занятий на макетах или в тестовой зоне Подготовка документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации Проведение проверки готовности персонала к эксплуатации системы защиты информации автоматизированной системы Подготовка документов, определяющих правила и процедуры контроля обеспеченности уровня защищенности информации,		Организация работы малых коллективов исполнителей. Участие в совершенствовании системы управления информационной безопасностью. Изучение и обобщение опыта работы других учреждений, организаций и предприятий в области защиты информации, в том числе информации ограниченного доступа.	

		содержащейся в информационной системе Подготовка документов, определяющих правила и процедуры выявления инцидентов, которые могут привести к сбоям или нарушению функционирования информационной системы и возникновению угроз безопасности информации Подготовка документов, определяющих правила и процедуры управления конфигурацией аттестованной информационной системой и системой защиты информации информационной системы			
	Анализ уязвимостей внедряемой системы защиты информации	Выбор и обоснование критериев эффективности функционирования защищенных автоматизированных систем Проведение анализа уязвимости программных и программно-аппаратных средств системы защиты информации автоматизированной системы Проведение экспертизы состояния защищенности		Контроль эффективности реализации политики информационной безопасности объекта защиты.	

		информации автоматизированных систем Уточнение модели угроз безопасности информации автоматизированной системы Проведение предварительных испытаний системы защиты информации автоматизированной системы Проведение анализа уязвимостей автоматизированных и информационных систем			

Наименование профессионального стандарта			**Наименование образовательной программы**		
СПЕЦИАЛИСТ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИИ (утв. приказом Минтруда России от 01.11.2016 № 599н) (действует до 28.02.2023)			**10.03.01 Информационная безопасность, профиль «Техническая защита информации»**		
ОТФ:	**ТФ:**	**ТД:**	**Типы задач профессиональной деятельности**	**Задачи профессиональной деятельности**	**Код и наименование профессиональной компетенции**
Проведение контроля защищенности информации	Проведение специальных исследований на побочные электромагнитные излучения и наводки технических средств обработки	Проведение специальных исследований на побочные электромагнитные излучения и наводки технических средств обработки информации Подготовка отчетных материалов по результатам специальных исследований на побочные электромагнитные	экспериментально-исследовательский	Проведение экспериментов по заданной методике, обработка и анализ их результатов.	ПК-3 проведение контроля защищенности информации

	информации	излучения и наводки технических средств обработки информации (предписаний на эксплуатацию технических средств и протоколов по результатам специальных исследований технических средств обработки информации)			
	Проведение контроля защищенности информации от утечки за счет побочных электромагнитных излучений и наводок	Проведение контроля защищенности информации от утечки за счет побочных электромагнитных излучений и наводок Подготовка отчетных материалов по результатам контроля защищенности информации от утечки за счет побочных электромагнитных излучений и наводок (протоколов оценки защищенности информации от утечки за счет побочных электромагнитных излучений и наводок)			
	Проведение контроля защищенности акустической речевой информации от	Проведение контроля защищенности акустической речевой информации от утечки по техническим каналам Подготовка отчетных			

	утечки по техническим каналам	материалов по результатам контроля защищенности акустической речевой информации от утечки по техническим каналам (протоколов оценки эффективности защиты акустической речевой информации от утечки по техническим каналам)			
	Проведение контроля защищенности информации от несанкционированного доступа	Проведение контроля защищенности информации от несанкционированного доступа и специальных воздействий Подготовка отчетных материалов по результатам контроля защищенности информации от несанкционированного доступа и специальных воздействий		Проведение вычислительных экспериментов с использованием стандартных программных средств.	
Наименование профессионального стандарта			**Наименование образовательной программы**		
Специалист по защите информации в автоматизированных системах (утв. Приказом Минтруда России от 14.09.2022 N 525н) (действует с 01.03.2023)			**10.03.01 Информационная безопасность, профиль «Техническая защита информации»**		
ОТФ:	**ТФ:**	**ТД:**	**Типы задач профессиональной деятельности**	**Задачи профессиональной деятельности**	**Код и наименование профессиональной компетенции**
Обеспечение защиты	Управление защитой	Анализ воздействия изменений конфигурации	эксплуатационный	Установка, настройка,	ПК-1 обеспечение защиты информации

информации в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости, в процессе их эксплуатации	информации в автоматизированных системах	автоматизированной системы на ее защищенность Составление комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе Оценка последствий от реализации угроз безопасности информации в автоматизированной системе Анализ изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации		эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований.	в автоматизированных системах в процессе их эксплуатации
	Обеспечение работоспособности систем защиты информации при возникновении нештатных ситуаций	Обнаружение неисправностей в работе системы защиты информации автоматизированной системы Устранение неисправностей в работе системы защиты информации автоматизированной системы Резервирование программного обеспечения, технических средств, каналов передачи данных автоматизированной системы управления на случай возникновения нештатных			

		ситуаций Создание альтернативных мест хранения и обработки информации на случай возникновения нештатных ситуаций Восстановление после сбоев и отказов программного обеспечения автоматизированных систем			
	Администрирование систем защиты информации автоматизированных систем	Установка обновлений программного обеспечения автоматизированной системы Выполнение установленных процедур обеспечения безопасности информации с учетом требования эффективного функционирования автоматизированной системы Управление полномочиями доступа пользователей автоматизированной системы Информирование пользователей о правилах эксплуатации автоматизированной системы с учетом требований по защите информации Проведение занятий с персоналом по работе с системой защиты информации		Администрирование подсистем информационной безопасности объекта.	

		автоматизированной системы, включая проведение практических занятий с персоналом на макетах или в тестовой зоне Внесение изменений в эксплуатационную документацию и организационно-распорядительные документы по системе защиты информации автоматизированной системы			
	Диагностика систем защиты информации автоматизированных систем	Обнаружение инцидентов в процессе эксплуатации автоматизированной системы Идентификация инцидентов в процессе эксплуатации автоматизированной системы Оценка защищенности автоматизированных систем с помощью типовых программных средств Устранение последствий инцидентов, возникших в процессе эксплуатации автоматизированной системы Расчет показателей эффективности защиты информации, обрабатываемой в автоматизированных системах		Участие в проведении аттестации объектов информатизации по требованиям безопасности информации и аудите информационной безопасности автоматизированных систем.	

		Инструментальный контроль показателей эффективности защиты информации, обрабатываемой в автоматизированных системах			
	Мониторинг защищенности информации в автоматизированных системах	Выработка рекомендаций для принятия решения о модернизации системы защиты информации автоматизированной системы Выработка рекомендаций для принятия решения о повторной аттестации автоматизированной системы или о проведении дополнительных аттестационных испытаний Выявление угроз безопасности информации в автоматизированных системах Принятие мер защиты информации при выявлении новых угроз безопасности информации Анализ недостатков в функционировании системы защиты информации автоматизированной системы Устранение недостатков в функционировании системы защиты информации автоматизированной системы			

	Аудит защищенности информации в автоматизированных системах	Оценка информационных рисков безопасности информации в автоматизированной системе Обоснование и контроль результатов управленческих решений в области безопасности информации автоматизированных систем Экспертиза состояния защищенности информации автоматизированных систем Обоснование критериев эффективности функционирования защищенных автоматизированных систем			
	Установка и настройка средств защиты информации в автоматизированных системах	Входной контроль качества комплектующих изделий системы защиты информации автоматизированной системы Осуществление автономной наладки технических и программных средств системы защиты информации автоматизированной системы Проведение приемочных испытаний системы защиты информации автоматизированной системы Внесение в эксплуатационную документацию изменений,	эксплуатационный	Установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований.	ПК-1 обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации

		направленных на устранение недостатков, выявленных в процессе испытаний			
	Разработка организационно-распорядительных документов по защите информации в автоматизированных системах	Определение правил и процедур управления системой защиты информации автоматизированной системы Определение правил и процедур выявления инцидентов Определение правил и процедур мониторинга обеспечения уровня защищенности информации автоматизированной системы Определение правил и процедур защиты информации при выводе автоматизированной системы из эксплуатации Определение правил и процедур реагирования на инциденты в автоматизированной системе	организационно-управленческий	Осуществление организационно-правового обеспечения информационной безопасности объекта защиты.	ПК-2 внедрение систем защиты информации автоматизированных систем
	Внедрение организационных мер по защите информации в автоматизированных системах	Проведение проверки полноты описания в организационно-распорядительных документах на автоматизированную систему действий персонала по реализации организационных мер защиты информации		Организация работы малых коллективов исполнителей.	
				Участие в совершенствовании системы управления информационной безопасностью.	

		Проведение занятий с персоналом по работе с системой защиты информации автоматизированной системы, включая проведение практических занятий на макетах или в тестовой зоне Подготовка документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации Проведение проверки готовности персонала к эксплуатации системы защиты информации автоматизированной системы Подготовка документов, определяющих правила и процедуры контроля обеспеченности уровня защищенности информации, содержащейся в информационной системе Подготовка документов, определяющих правила и процедуры выявления инцидентов, которые могут привести к сбоям или нарушению		Изучение и обобщение опыта работы других учреждений, организаций и предприятий в области защиты информации, в том числе информации ограниченного доступа.	

		функционирования информационной системы и возникновению угроз безопасности информации Подготовка документов, определяющих правила и процедуры управления конфигурацией аттестованной информационной системы и системы защиты информации информационной системы			
	Анализ уязвимостей внедряемой системы защиты информации	Выбор и обоснование критериев эффективности функционирования защищенных автоматизированных систем Проведение анализа уязвимости программных и программно-аппаратных средств системы защиты информации автоматизированной системы Проведение экспертизы состояния защищенности информации автоматизированных систем Уточнение модели угроз безопасности информации автоматизированной системы Проведение предварительных испытаний системы защиты информации		Контроль эффективности реализации политики информационной безопасности объекта защиты.	

		автоматизированной системы Проведение анализа уязвимостей автоматизированных и информационных систем			
Специалист по технической защите информации (утв. Приказом Минтруда России от 09.08.2022 N 474н) (действует с 01.03.2023)			**10.03.01 Информационная безопасность, профиль «Техническая защита информации»**		
ОТФ:	**ТФ:**	**ТД:**	**Типы задач профессиональной деятельности**	**Задачи профессиональной деятельности**	**Код и наименование профессиональной компетенции**
Проведение контроля защищенности информации	Проведение специальных исследований на побочные электромагнитные излучения и наводки технических средств обработки информации	Измерение побочных электромагнитных излучений технических средств обработки информации в различных режимах их работы Измерение наводок побочных электромагнитных излучений технических средств обработки информации в различных режимах их работы Подготовка отчетных материалов по результатам специальных исследований на побочные электромагнитные излучения и наводки технических средств обработки информации (предписаний на эксплуатацию технических средств и протоколов по результатам специальных	экспериментально-исследовательский	Проведение экспериментов по заданной методике, обработка и анализ их результатов.	ПК-3 проведение контроля защищенности информации

		исследований технических средств обработки информации)			
	Проведение контроля защищенности информации от утечки за счет побочных электромагнитных излучений и наводок	Проверка состояния организации работ и выполнения требований по защите информации от утечки за счет побочных электромагнитных излучений и наводок Испытания (с использованием технических средств) с целью проверки защищенности информации от утечки за счет побочных электромагнитных излучений и наводок Подготовка отчетных материалов по результатам контроля защищенности информации от утечки за счет побочных электромагнитных излучений и наводок (протоколов оценки защищенности информации от утечки за счет побочных электромагнитных излучений и наводок)			
	Проведение контроля защищенности акустической речевой	Проверка состояния организации работ и выполнения требований по защите акустической речевой информации от утечки по			

	информации от утечки по техническим каналам	техническим каналам Испытания (с использованием технических средств) с целью проверки защищенности акустической речевой информации от утечки по техническим каналам Подготовка отчетных материалов по результатам контроля защищенности акустической речевой информации от утечки по техническим каналам (протоколов оценки эффективности защиты акустической речевой информации от утечки по техническим каналам)			
	Проведение контроля защищенности информации от несанкционированного доступа	Проверка состояния организации работ и выполнения требований по защите информации от несанкционированного доступа Испытания автоматизированной системы на соответствие требованиям по защите информации от несанкционированного доступа Подготовка отчетных материалов по результатам		Проведение вычислительных экспериментов с использованием стандартных программных средств.	

		контроля защищенности информации от несанкционированного доступа и специальных воздействий			