МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Кузбасский государственный технический университет имени Т. Ф. Горбачева»

Институт информационных технологий, машиностроения и автотранспорта

ПОДПИСАНО ЭП КУЗГТУ

Должность: Ректор
Дата:

В.В. Меркурьев

Основная профессиональная образовательная программа

Направление подготовки / специальность 10.04.01 Информационная безопасность
Специализация / направленность (профиль) Организация и технология защиты информации

Присваиваемая квалификация
"Магистр"

Формы обучения
очная

Год набора 2026

ПОДПИСАНО ЭП КУЗГТУ

Председатель учебно-методической комиссии
по направлению подготовки (специальности)
10.04.01 Информационная безопасность

Дата:

Е.В. Прокопенко

Кемерово 2026 г.

cde9fa65dfb5e9a6d20ff04a423d1ffe

СОДЕРЖАНИЕ

1. **Характеристики основной профессиональной образовательной программы**
1.1 Миссия и цели ОПОП
1.2 Квалификация, присваиваемая выпускникам
1.3 Задачи профессиональной деятельности выпускника
1.4 Специализация / направленность (профиль) основной профессиональной образовательной программы
1.5 Планируемые результаты освоения ОПОП
1.6 Планируемые результаты обучения по каждой дисциплине (модулю) и практике - знания, умения, навыки и (или) опыт деятельности (индикаторы достижения компетенции), характерезующие этапы формирования компетенций и обеспечивающие достижение планируемых результатов освоения ОПОП
1.7 Сведения о профессорско-преподавательском составе, необходимом для реализации образовательной программы
2. **Иные сведения**
2.1 Перечень методов, средств обучения и образовательных технологий
2.2 Нормативные документы для разработки образовательной программы
2.3 Требования к материально-техническому и учебно-методическому обеспечению образовательной программы
2.4 Особенности организации образовательной деятельности для обучающихся с ограниченными возможностями здоровья
2.5 Государственная итоговая аттестация
3. **Рабочая программа воспитания и календарный план воспитательной работы**
4. **Внесение изменений**

1. Характеристики основной профессиональной образовательной программы

1.1 Миссия и цели ОПОП

Миссия реализации образовательной программы состоит в комплексной и системной подготовке обучающихся, владеющих знаниями и комплексом методологических, технологических и инструментальных средств, обладающих совокупностью необходимых компетенций для успешной работы в различных сферах деятельности, связанных анализом и эксплуатацией средств и систем защиты информационных систем, доказательным анализом и обеспечением защищённости компьютерных систем от вредоносных программно-технических и информационных воздействий в условиях нарастания угроз в информационной сфере.

Область (области) профессиональной деятельности и (или) сфера (сферы) профессиональной деятельности выпускников, освоивших ОПОП ВО по направлению подготовки 10.04.01 «Информационная безопасность», направленность (профиль) «Организация и технология защиты информации», включает:

06 Связь, информационные и коммуникационные технологии (в сферах: защиты информации в компьютерных системах и сетях, автоматизированных системах, системах и сетях электросвязи; технической защиты информации; защиты значимых объектов критической информационной инфраструктуры, информационно-аналитических систем безопасности);

Объектами профессиональной деятельности выпускников, освоивших программу специалитета, являются:

1. фундаментальные и прикладные проблемы информационной безопасности;
2. объекты информатизации, информационные ресурсы и информационные технологии, компьютерные, автоматизированные, телекоммуникационные, информационные и информационно-аналитические системы;
3. средства и технологии обеспечения информационной безопасности и защиты информации;
4. экспертиза, сертификация и контроль защищенности информации и объектов информатизации;
5. методы и средства проектирования, моделирования и экспериментальной отработки систем, средств и технологий обеспечения информационной безопасности объектов информатизации;
6. организация и управление информационной безопасностью;

Срок получения образования по каждой форме обучения: Очная форма обучения: 2 года.

Объем образовательной программы по каждой форме обучения: Очная форма обучения: 120 ЗЕ

Объем образовательной программы по каждой форме обучения, реализуемый за один учебный год: 60 ЗЕ

Применение электронного обучения, дистанционных образовательных технологий: нет

Цели:

Формирование у обучающихся компетенций в соответствии с требованиями федерального государственного образовательного стандарта.

Получение выпускниками высшего образования с учетом профессиональных стандартов, позволяющего выпускнику успешно работать в избранной сфере деятельности.

Формирование социально-личностных качеств обучающихся, способствующих укреплению нравственности, развитию общекультурных потребностей, творческих способностей, социальной адаптации, коммуникативности, толерантности, настойчивости в достижении цели, готовности принимать решения и профессионально действовать.

1.2 Квалификация, присваиваемая выпускникам

Присваиваемая квалификация – Магистр.

Тип(ы) решаемых задач (вид(ы) профессиональной деятельности):

1) организационно-управленческий

2) проектный

Из них основные:

1) организационно-управленческий

2) проектный

Типы решаемых задач:

1. организационно-управленческий
2. проектный

Достижение целей в подготовке магистров по ОПОП соответствует следующим профессиональным стандартам:

№ п/п	Реквизиты профессионального стандарта
1	06.034 Профессиональный стандарт «Специалист по технической защите информации» утвержден приказом Министерства труда и социальной защиты Российской Федерации от 09.08.2022 № 474н

Перечень профессиональных стандартов, обобщённых трудовых функций и трудовых функций, имеющих отношение к профессиональной деятельности выпускника программы магистратуры по направлению подготовки 10.04.01 Информационная безопасность, направленность (профиль) «Организация и технология защиты информации»:

Профессиональный стандарт	Обобщенные трудовые функции			Трудовые функции		
Заимствовано из оригинала:	код	наименование	уровень квалификации	код	наименование	уровень (подуровень) квалификации
06.034 Специалист по технической защите информации	H	Проектирование объектов информатизации в защищенном исполнении	7	H/01.7	Проектирование объектов вычислительной техники (далее - ОВТ) в защищенном исполнении	7
06.034 Специалист по технической защите информации	H	Проектирование объектов информатизации в защищенном исполнении	7	H/02.7	Проектирование выделенных (защищаемых) помещений	7
06.034 Специалист по технической защите информации	L	Организация и проведение работ по защите информации в организации	7	L/01.7	Аналитическое обоснование необходимости создания системы защиты информации в организации	7
06.034 Специалист по технической защите информации	L	Организация и проведение работ по защите информации в организации	7	L/02.7	Ввод в эксплуатацию системы защиты информации в организации	7
06.034 Специалист по технической защите информации	L	Организация и проведение работ по защите информации в организации	7	L/03.7	Сопровождение системы защиты информации в ходе ее эксплуатации	7

Соответствие обобщенных трудовых функций, трудовых функций, трудовых действий из профессионального стандарта 06.034 «Специалист по технической защите информации» типам задач профессиональной деятельности из ФГОС ВО.

Обобщенные трудовые функции (из ПС)	Трудовые функции (из ПС)	Трудовые действия (из ПС)	Профессиональные компетенции (установленные ОО на основании ПС)	Тип задач профессиональной деятельности (из ФГОС ВО)
Проектирование объектов информатизации в защищенном исполнении	Проектирование объектов вычислительной техники (далее - ОВТ) в защищенном исполнении	Предпроектное обследование ОВТ	ПК-1 Владеет методикой проведения предпроектного обследования объектов информатизации и выделенных(защищаемых) помещений	проектный

Обобщенные трудовые функции (из ПС)	Трудовые функции (из ПС)	Трудовые действия (из ПС)	Профессиональные компетенции (установленные ОО на основании ПС)	Тип задач профессиональной деятельности (из ФГОС ВО)
Проектирование объектов информатизации в защищенном исполнении	Проектирование объектов вычислительной техники (далее - ОВТ) в защищенном исполнении	Разработка модели угроз безопасности информации, обрабатываемой на ОВТ	ПК-2 Способен приводить аналитическое обоснование необходимости создания систем защиты информации	проектный
Проектирование объектов информатизации в защищенном исполнении	Проектирование объектов вычислительной техники (далее - ОВТ) в защищенном исполнении	Разработка эксплуатационной документации на ОВТ в защищенном исполнении, а также организационно-распорядительной документации по защите информации на ОВТ	ПК-1 Владеет методикой проведения предпроектного обследования объектов информатизации и выделенных(защищаемых) помещений	организационно-управленческий
Проектирование объектов информатизации в защищенном исполнении	Проектирование выделенных (защищаемых) помещений	Предпроектное обследование выделенного (защищаемого) помещения	ПК-1 Владеет методикой проведения предпроектного обследования объектов информатизации и выделенных(защищаемых) помещений	проектный
Проектирование объектов информатизации в защищенном исполнении	Проектирование выделенных (защищаемых) помещений	Разработка эксплуатационной документации на систему защиты информации выделенного (защищаемого) помещения, а также организационно-распорядительной документации по защите информации в выделенном (защищаемом) помещении	ПК-1 Владеет методикой проведения предпроектного обследования объектов информатизации и выделенных(защищаемых) помещений	организационно-управленческий
Организация и проведение работ по защите информации в организации	Разработка аналитического обоснования необходимости создания системы защиты информации в организации в организации	Разработка аналитического обоснования необходимости создания системы защиты информации в организации	ПК-1 Владеет методикой проведения предпроектного обследования объектов информатизации и выделенных(защищаемых) помещений	организационно-управленческий
Организация и проведение работ по защите информации в организации	Аналитическое обоснование необходимости создания системы защиты информации в организации	Разработка модели угроз безопасности информации в организации	ПК-1 Владеет методикой проведения предпроектного обследования объектов информатизации и выделенных(защищаемых) помещений	организационно-управленческий
Организация и проведение работ по защите информации в организации	Ввод в эксплуатацию системы защиты информации в организации	Организация проведения инструктажа руководящего состава и обучения персонала по вопросам технической защиты информации	ПК-5 Способен организовывать и проводить приемочные испытания СЗИ, вводить в эксплуатацию СЗИ	организационно-управленческий
Организация и проведение работ по защите информации в организации	Ввод в эксплуатацию системы защиты информации в организации	Организация приемочных испытаний системы защиты информации	ПК-5 Способен организовывать и проводить приемочные испытания СЗИ, вводить в эксплуатацию СЗИ	организационно-управленческий
Организация и проведение работ по защите информации в организации	Сопровождение системы защиты информации в ходе ее эксплуатации	Организация мероприятий по выводу из эксплуатации систем информатизации и по утилизации их элементов	ПК-5 Способен организовывать и проводить приемочные испытания СЗИ, вводить в эксплуатацию СЗИ	организационно-управленческий

Профессиональные компетенции, определенные на основе анализа требований к профессиональным компетенциям, предъявляемых к выпускникам на рынке труда, обобщения отечественного и зарубежного опыта, проведения консультаций с ведущими работодателями, объединениями работодателей отрасли, в которой востребованы выпускники, иных источников.

Код компетенции	Название компетенции	Тип задач профессиональной деятельности
ПК-3	Владеет нормативно-методической базой обеспечения защиты сведений, составляющих государственную тайну	организационно-управленческий
ПК-4	Способен организовывать и сопровождать аттестацию объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации	организационно-управленческий

1.3 Задачи профессиональной деятельности выпускника

Выпускник по направлению подготовки / специальности 10.04.01 «Информационная безопасность», специализация / направленность (профиль) «Организация и технология защиты информации» должен решать следующие профессиональные задачи в соответствии с типом(ами) задач профессиональной деятельности или видом(ами) профессиональной деятельности, на которые ориентирована образовательная программ:

Тип задач - проектный:

системный анализ прикладной области, выявление угроз и оценка уязвимости информационных систем, разработка требований и критериев оценки информационной безопасности;
обоснование выбора состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе отечественных и международных стандартов;
разработка систем, комплексов, средств и технологий обеспечения информационной безопасности;
разработка программ и методик испытаний средств и систем обеспечения информационной безопасности.

Тип задач - организационно-управленческий:

организация работы коллектива исполнителей, принятие управленческих решений, определение порядка выполнения работ;
организация управления информационной безопасностью;
организация работы по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации (далее – ФСБ России), Федеральной службы по техническому и экспортному контролю Российской Федерации (далее ФСТЭК России);
организация и выполнение работ вводу в эксплуатацию систем и средств обеспечения информационной безопасности;
разработка проектов организационно-распорядительных документов, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности.

1.4 Специализация / направленность (профиль) основной профессиональной образовательной программы

Специализация / направленность (профиль) основной профессиональной образовательной программы - Организация и технология защиты информации.

1.5 Планируемые результаты освоения ОПОП

Результаты освоения ОПОП магистратуры определяются приобретаемыми выпускником компетенциями.

В результате освоения программы магистратуры выпускник должен обладать следующими компетенциями:

Компетенции выпускников формируемые ОПОП по направлению

Код и содержание компетенции	Индикаторы достижения компетенции	Результаты обучения
Общепрофессиональные компетенции(ОПК)		
ОПК-1 Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;	Обосновывает требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание.	Знает принципы разработки защищенных информационных систем различного применения и степени сложности. Знает методики выявления угроз и оценки уязвимостей информационных систем. Знает методы и средства обеспечения информационной безопасности, а также нормативную базу регламентирующую классификацию данных средств. Знает типовые требования к разработке средств защиты, направленные на снижение рисков информационной безопасности. Умеет обосновывать требования к процессам и технологиям обеспечения информационной безопасности объектов критической информационной инфраструктуры. Умеет осуществлять выбор подсистем, реализующих технологии обеспечения информационной безопасности для объектов критической информационной инфраструктуры. Умеет обосновывать требования к мерам обеспечения информационной безопасности объектов критической информационной инфраструктуры. Умеет составлять техническое задание по разработке систем, комплексов, средств и технологий обеспечения информационной безопасности. Умеет настраивать средства защиты информации в соответствии с требованиями к объекту защиты с целью снижения рисков информационной безопасности Владеть навыками разработки комплексной инфраструктуры защищенной информационной системы, навыками разработки проектов нормативных и правовых актов предприятия, учреждения, организации, регламентирующих деятельность по обеспечению ИБ.

ОПК-1 Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;	Способен обосновывать требования к системе обеспечения информационной безопасности .	Знает технологии обеспечения информационной безопасности. Знает основные виды уязвимостей систем и угрозы информационной безопасности. Знает методы и средства обеспечения информационной безопасности, а также нормативную базу регламентирующую классификацию данных средств. Умеет обосновывать выбор средств защиты информации для противодействия конкретным угрозам. Умеет осуществлять подбор средств защиты информации в соответствии с заданными критериями. Умеет обосновывать требования к мерам обеспечения информационной безопасности в соответствии с нормативной базой. Умеет составлять техническое задание по обеспечению информационной безопасности на объекте с использованием сертифицированных ФСТЭК средств защиты информации. Владеет опытом настройки средства защиты информации в соответствии с требованиями к объекту защиты с целью снижения рисков информационной безопасности.
ОПК-1 Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;	Обосновывает требования к системе обеспечения информационной безопасности и способен разработать проект технического задания на ее создание.	Иметь опыт формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем. Уметь определять информационные ресурсы, подлежащие защите информации, угрозы безопасности информации. Владеть профессиональной терминологией в области обеспечения безопасности персональных данных; методами мониторинга и аудита, выявления угроз и управления информационной безопасностью. Знать уязвимости информационных ресурсов, возможные угрозы безопасности информации, информационные процессы объектов.

ОПК-1 Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;	Обосновывает требования к системе обеспечения информационной безопасности и разрабатывает проекты технического задания на ее создание.	Знать основные принципы организации технического, программного и информационною обеспечения защищенных информационных систем; основные механизмы информационной безопасности и типовые процессы управления этими механизмами в информационной системе; основные угрозы безопасности информации и модели нарушителя в информационных системах; принципы формирования политики информационной безопасности в информационных системах; методы аттестации уровня защищенности информационных систем; основные методы управления информационной безопасностью; основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем. Уметь строить системы обеспечения информационной безопасности в различных условиях функционирования защищаемых информационных систем; разрабатывать модели угроз и нарушителей информационной безопасности информационных систем; разрабатывать частные политики информационной безопасности информационных систем; контролировать эффективность принятых мер по реализации частных политик информационной безопасности информационных систем; оценивать информационные риски в информационных системах; разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных систем; составлять аналитические обзоры по вопросам обеспечения информационной безопасности информационных систем; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности. Владеть методами и средствами выявления угроз безопасности информационным системам; навыками выбора и обоснования критериев эффективности функционирования защищенных информационных систем; навыками участия в экспертизе состояния защищенности информации на объекте защиты; методами управления информационной безопасностью информационных систем; методами опенки информационных рисков; методами организации и управления деятельностью служб защиты информации на предприятии; навыками управления информационной безопасностью простых объектов.

ОПК-2 Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности;	Разрабатывает требования к средствам и методам контроля проектируемой системы (подсистемы либо компонента системы) обеспечения информационной безопасности.	Знает принципы построения систем на базе IoTустройств, а также способы их эффективной реализации; существующие технологии в области Интернета вещей; стандарты реализации интерфейсов подключаемых устройств; стандарты информационного взаимодействия систем. Знает типовые средства и методы защиты информации в локальных и глобальных вычислительных сетях; требования НПА и стандартов по разработке моделей угроз информационной безопасности; наиболее распространенные уязвимости IoTустройств и протоколов передачи данных; средства обеспечения информационной безопасности IoT-систем; принципы построения защищенных телекоммуникационных систем; механизмы реализации атак в сетях Интернета вещей; Умеет проводить анализ защищенности IoT-систем; Разрабатывать модели угроз для систем Интернета Вещей. Умеет проводить первичную настройку и проверку функционирования СССЭ, средств и систем защиты СССЭ от НСД; разбираться в существующих IoT-технологиях и применять их к конкретным сценариям; внедрять типовые решения по информационной безопасности IoT-систем; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты в соответствии с требованиями нормативно правовых актов и нормативных методических документов. Владеет способами конфигурировать параметры системы защиты информации автоматизированной системы в соответствии с ее эксплуатационной документацией; работать с документацией прилагаемой разработчиком устройства; обнаруживать типовые уязвимости IoT систем. Может формировать требования и разрабатывать спецификации для проектируемой системы на базе IoTустройств; планировать разработку сложных системы на базе IoT-устройств; проводить выбор эффективных способов реализации структур системы на базе IoTустройств при решении профессиональных задач.

ОПК-2 Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности;	Способен разработать технические проекты систем (подсистем) либо компонента системы обеспечения информационной безопасности.	Иметь опыт разработки технических проектов систем (подсистем) либо компонента системы обеспечения информационной безопасности. Уметь отечественные и зарубежные стандарты в области компьютерной безопасности и информационной безопасности объектов для проектирования, разработки и оценки защищенности компьютерных систем. Владеть методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов. Знать основы организации защиты государственной тайны и конфиденциальной информации; методы анализа информационной безопасности объектов и систем; стандарты в области информационной безопасности.
ОПК-2 Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности;	Разрабатывает технический проект системы обеспечения информационной безопасности, а также их компонент(подсистемы).	Знать основные принципы разработки политики информационной безопасности на предприятии, принципы анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности, современную аппаратно-программную базу компьютерной техники для решения задач защиты информации. Уметь применять комплексный подход к обеспечению информационной безопасности объекта защиты, проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности, применять программные средства системного, прикладного и средства системного, специального назначения, инструментальные средства, языки и системы программирования для решения задач защиты информации. Владеть основными методами обеспечения информационной безопасности объекта защиты, методами технико-экономического обоснования проектных решений, методами и средствами системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения задач защиты информации.

ОПК-2 Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности;	Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности .	Знает принципы эксплуатации средств защиты информации. Знает методы тестирования средств защиты информационной безопасности. Умеет осуществлять настройку режимов работы средств защиты информации в соответствии с определенными моделями угроз. Умеет разрабатывать сценарии тестирования средств защиты информации. Умеет разрабатывать требования к средствам защиты информации. Умеет управлять средствами защиты информации в соответствии с требованиями к объекту защиты. Имеет опыт разработки требования к средствам и методам контроля проектируемой системы (подсистемы либо компонента системы) обеспечения информационной безопасности.
ОПК-2 Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности;	Разрабатывает технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности.	Знает принципы организации и этапы разработки системы (подсистемы либо компонента системы) обеспечения информационной безопасности объектов критической информационной инфраструктуры. Знает методики испытаний средств и систем обеспечения информационной безопасности. Умеет составлять требования и критерии оценки информационной безопасности. Умеет разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности объектов критической информационной инфраструктуры. Умеет разрабатывать требования к средствам и методам контроля проектируемой системы (подсистемы либо компонента системы) обеспечения информационной безопасности объектов критической информационной инфраструктуры. Умеет разрабатывать и реализовывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности объектов критической информационной инфраструктуры. Владеть навыками технических проектов систем (подсистемы либо компонента системы) обеспечения информационной безопасности.

ОПК-3 Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности;	Способен разработать проекты организационно-распорядительных документов по обеспечению информационной безопасности.	Иметь опыт разработки проектов организационно-распорядительных документов по обеспечению информационной безопасности. Уметь осуществлять подготовку технических заданий на построение и проектирование информационных и аналитических систем; осуществлять подготовку организационно-распорядительной документации (инструкции, приказы, распоряжения) регламентирующей эксплуатацию информационных систем. Владеть навыками оформления рабочей технической документации. Знать требования основных действующих государственных стандартов (ГОСТ) регламентирующие построение, проектирование и эксплуатацию информационных и аналитических систем.
ОПК-3 Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности;	Разрабатывает проекты организационно-распорядительных документов по обеспечению информационной безопасности.	Знать источники правовой информации, виды нормативных правовых актов, стандарты в области информационной безопасности. Уметь анализировать, изучать и обобщать правовую информацию, определять релевантные для профессиональной деятельности нормативные акты, использовать нормативные и методические документы при оформлении технической документации. Владеть навыками обоснования своих решений на основе действующего законодательства, навыками поиска требуемой информации используя нормативные правовые акты, навыками подготовки проектов организационно-распорядительных документов по обеспечению информационной безопасности.
ОПК-3 Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности;	Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности	Знает нормативную и правовую базу в области управления информационной безопасностью объектов критической информационной инфраструктуры. Знает отечественные и зарубежные стандарты в области управления информационной безопасностью объектов критической информационной инфраструктуры. Знает структуру политик обеспечения информационной безопасности объектов критической информационной инфраструктуры и требования к их содержанию Умеет разрабатывать проекты нормативных и организационно-распорядительных документов по обеспечению информационной безопасности объектов критической информационной инфраструктуры. Умеет разрабатывать политику информационной безопасности объектов критической информационной инфраструктуры различных уровней Владеет навыками разработки политики информационной безопасности различных уровней

ОПК-4 Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок;	Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок	Знает основные формы, методы и приемы научного исследования области безопасности объектов критической информационной инфраструктуры. Умеет составлять план научного исследования в области безопасности объектов критической информационной инфраструктуры и проводить деятельность в соответствии с составленным планом. Умеет разрабатывать программу разработки компонентов средств защиты информации для объектов критической информационной инфраструктуры. Демонстрирует способности анализа наборов данных при помощи различных сред их анализа с наглядной визуализацией получаемых результатов
ОПК-4 Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок;	Осуществляет сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок.	Иметь опыт сбора, обработки и анализа научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок. Уметь проектировать и сопровождать типовые специализированные автоматизированные информационные системы, локальные сети; осуществлять подготовку технико-экономических обоснований соответствующих проектных решений. Владеть навыками определения затрат компании на информационную безопасность и проведения зависимости между затратами и уровнем защищенности. Знать методы проектирования автоматизированных систем; основные принципы проектного управления.
ОПК-5 Способен проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи.	Проводит научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи.	Иметь опыт оформления научно-технических отчетов, обзоров, результатов выполненных исследований, научных докладов и статей. Уметь разбираться в лабораторном оборудовании по профилю своей деятельности и работать с оборудованием для проведения экспериментов, применять методики, обрабатывать результаты, проводить оценку погрешности, проводить экспериментально-исследовательские работы системы защиты информации. Владеть навыками выполнения расчетов, обработки результатов экспериментов, оценки погрешностей и достоверности результатов, навыками проведения экспериментально-исследовательских работ системы защиты информации. Знать основные принципы экспериментальных исследований, соотношение теоретического и экспериментального знания, методику проведения экспериментов.

ОПК-5 Способен проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи.	Способен проводить научные исследования.	Знать методы научных исследований; организацию научных исследований и этапы их проведения; процедуры разработки и проектирования новых технических объектов; теоретические исследования; построение моделей физических процессов и объектов; проведение экспериментальных исследования и обработка их результатов. Уметь применять методы научных исследований ; организовывать научные исследования; проводить экспериментальные исследования и обрабатывать их результаты. Владеть методами научных исследований ; организации научных исследований; навыками экспериментальных исследований и обработки их результатов.
Профессиональные компетенции(ПК)		
ПК-1 Владеет методикой проведения предпроектного обследования объектов информатизации и выделенных(защищаемых) помещений	Владеет методикой проведения предпроектного обследования объектов информатизации и выделенных защищаемых помещений.	Иметь опыт проведения предпроектного обследования объектов информатизации и выделенных защищаемых помещений. Уметь выполнять проектирование и разработку систем, комплексов, средств и технологий обеспечения информационной безопасности. Владеть навыками работы в среде CASE-средств анализа и проектирования систем навыками использования в практической деятельности новых знаний и умений. Знать методологию проектирования систем, комплексов, средств и технологий обеспечения информационной безопасности, необходимые для разработки систем, комплексов, средств и технологий обеспечения информационной безопасности.
ПК-1 Владеет методикой проведения предпроектного обследования объектов информатизации и выделенных(защищаемых) помещений	Владеет методикой проведения предпроектного обследования объектов информатизации и выделенных(защищаемых) помещений	Знает содержание и порядок деятельности персонала объектов критической информационной инфраструктуры и ее частей. Знает нормативную базу, регламентирующую процессы обеспечения информационной безопасности объектов критической информационной инфраструктуры и ее частей. Умеет разрабатывать организационно-распорядительные документы по обеспечению безопасности значимых объектов критической информационной инфраструктуры. Владеет техническими мерами обеспечения безопасности значимых объектов критической информационной инфраструктуры.

ПК-2 Способен приводить аналитическое обоснование необходимости создания систем защиты информации	Приводит аналитическое обоснование необходимости создания систем защиты информации.	Иметь опыт приведения аналитическое обоснование необходимости создания систем защиты информации. Уметь проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты. Владеть навыками обеспечения информационной безопасностью объектов защиты. Знать российские и международные стандарты в области информационной безопасности.
ПК-2 Способен приводить аналитическое обоснование необходимости создания систем защиты информации	Способен приводить аналитическое обоснование необходимости создания систем защиты информации	Знает общие принципы организации защиты объектов критической информационной инфраструктуры и ее частей. Умеет организовывать защиту объектов критической информационной инфраструктуры и ее частей с учетом действующих нормативных и методических документов. Владеет методикой определения категории объектов критической информационной инфраструктуры.
ПК-3 Владеет нормативно-методической базой обеспечения защиты сведений, составляющих государственную тайну	Владеет нормативно-методической базой обеспечения защиты сведений, составляющих государственную тайну.	Знать нормативно-правовое обеспечение сертификации технических и программных средств защиты информации, правила лицензирования и сертификации в области защиты информации; порядок проведения аттестации объектов информационной защиты. Уметь применять стандарты и другие нормативные документы при оценке, контроле качества и сертификации; определять рациональные способы и средства защиты информации на объекте информатизации; организовать мероприятия по защите информации на объекте информатизации. Владеть схемами сертификации и правилами декларирования соответствия; признаками обязательной и добровольной сертификации.
ПК-3 Владеет нормативно-методической базой обеспечения защиты сведений, составляющих государственную тайну	Владеет нормативной базой обеспечения области защиты государственной тайны, информационной безопасности, соблюдения режима секретности.	Знать требования правовых актов в области защиты государственной тайны и информационной безопасности, режима секретности Уметь соблюдать в профессиональной деятельности требования правовых актов в области защиты информации и сведений составляющих государственную тайну Владеть навыками обеспечения соблюдения режима секретности

ПК-3 Владеет нормативно-методической базой обеспечения защиты сведений, составляющих государственную тайну	Владеет нормативно-методической базой обеспечения защиты сведений, составляющих государственную тайну.	Иметь опыт подготовки нормативно-методической базы по защите сведений, составляющих государственную тайну. Уметь организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами. Владеть знаниями законодательных и правовых актов в области безопасности; правилами составления локальных нормативных актов и регламентов в области информационной безопасности. Знать основные принципы организации систем, средств и технологий обеспечения информационной безопасности.
ПК-3 Владеет нормативно-методической базой обеспечения защиты сведений, составляющих государственную тайну	Владеет нормативно-методической базой обеспечения защиты сведений, составляющих государственную тайну.	Иметь опыт подготовки нормативно-методической базы. Уметь использовать полученные знания в профессиональной деятельности. Владеть нормативно-методической базой обеспечения защиты сведений, составляющих государственную тайну. Знать нормативную базу для обеспечения защиты сведений, составляющих государственную тайну.
ПК-4 Способен организовывать и сопровождать аттестацию объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации	Организует и сопровождает аттестацию объектов вычислительной техники и выделенных защищаемых помещений на соответствие требованиям по защите информации.	Иметь опыт организации подготовки объектов вычислительной техники и выделенных (защищаемых) помещений к аттестации по требованиям безопасности информации. Уметь подготавливать объекты вычислительной техники и выделенные (защищаемые) помещения к аттестации по требованиям безопасности информации. Владеть методами подготовки объектов вычислительной техники и выделенных (защищаемых) помещений к аттестации. Знать порядок аттестации объектов информатизации на соответствие требованиям по защите информации.
ПК-4 Способен организовывать и сопровождать аттестацию объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации	Организует и сопровождает аттестацию объектов вычислительной техники и выделенных защищаемых помещений на соответствие требованиям по защите информации.	Иметь опыт организации и сопровождения аттестации объектов вычислительной техники и выделенных защищаемых помещений на соответствие требованиям по защите информации. Уметь проводить экспериментальные исследования защищенности объектов, разрабатывать требования к защите от утечек по техническим каналам. Владеть методами инструментального контроля защищенности объекта. Знать понятия контура безопасности, физические и математические методы исследования защищенности объектов; порядок проведения аттестации объектов информатизации по требованиям безопасности информации, требования стандартов и иных нормативно-технических документов по безопасности информации, утвержденных Гостехкомиссией России.

ПК-4 Способен организовывать и сопровождать аттестацию объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации	Способен организовывать и сопровождать аттестацию объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации.	Знает нормативную базу, регламентирующую процессы аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации. Умеет разрабатывать организационно-распорядительные документы по сопровождению процессов аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации. Имеет опыт организации аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации.
ПК-5 Способен организовывать и проводить приемочные испытания СЗИ, вводить в эксплуатацию СЗИ	Организует и проводит приемочные испытания СЗИ, вводит в эксплуатацию СЗИ.	Иметь опыт организации приемочных испытаний систем защиты информации. Уметь организовывать приемочные испытания системы защиты информации Владеть способами приемочных испытаний СЗИ, ввода в эксплуатацию СЗИ. Знать методы защиты информации от утечки, эксплуатационную документацию на систему защиты информации.
ПК-5 Способен организовывать и проводить приемочные испытания СЗИ, вводить в эксплуатацию СЗИ	Способен организовывать и проводить приемочные испытания СЗИ, вводить в эксплуатацию СЗИ	Нормативную базу регламентирующую приемочные испытания СЗИ при вводе в эксплуатацию СЗИ Умеет организовывать приемочные испытания системы защиты информации Методами организация приемочных испытаний системы защиты информации
ПК-5 Способен организовывать и проводить приемочные испытания СЗИ, вводить в эксплуатацию СЗИ	Способен организовывать и проводить приемочные испытания СЗИ, вводить в эксплуатацию СЗИ.	Нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации Уметь организовывать ввод системы защиты информации в эксплуатацию. Владеть навыками ввода системы защиты информации в эксплуатацию.
ПК-5 Способен организовывать и проводить приемочные испытания СЗИ, вводить в эксплуатацию СЗИ	Организует и проводит приемочные испытания СЗИ, вводит в эксплуатацию СЗИ.	Иметь опыт организации приемочных испытаний систем защиты информации. Уметь организовывать приемочные испытания системы защиты информации. Владеть способами приемочных испытаний СЗИ, ввода в эксплуатацию СЗИ. Знать методы защиты информации от утечки, эксплуатационную документацию на систему защиты информации.
ПК-6 Прогнозирует риски в информационной безопасности и управляет инцидентами информационной безопасности	Прогнозирует риски в информационной безопасности и управляет инцидентами информационной безопасности.	Иметь опыт анализа рисков в информационной безопасности и управлении инцидентами информационной безопасности. Уметь организовать процесс управления информационной безопасностью. Владеть навыками управления системой информационной безопасности. Знать порядок организации деятельности по управлению информационной безопасностью.

ПК-6 Прогнозирует риски в информационной безопасности и управляет инцидентами информационной безопасности	Прогнозирует риски в информационной безопасности и управляет инцидентами информационной безопасности.	Иметь опыт определения риски в информационной безопасности и управления инцидентами информационной безопасности. Уметь проводить качественную оценку рисков, определять вероятность реализации угрозы по отношению к информационному активу, определять уровень возможности успешной реализации угрозы с учетом текущего состояния ИБ, внедренных мер и средств защиты. Владеть методами разработки мер безопасности, контрмер и действий по каждой актуальной угрозе для снижения уровня риска, управлять инцидентами информационной безопасности. Знать количественный и качественный подходы к оценке рисков ИБ.
ПК-6 Прогнозирует риски в информационной безопасности и управляет инцидентами информационной безопасности	Способен построить моделей угроз информационной безопасности, выявлять и оценивать актуальности угроз информационной безопасности, построения их моделей для определения требований о защите информации	Знает общую информацию об угрозах и нарушителях безопасности информации компьютерных систем. Знает методику выявления и оценки актуальности угроз информационной безопасности, построения их моделей для определения требований о защите информации Умеет выявлять и оценивать актуальности угроз информационной безопасности, построения их моделей для определения требований о защите информации Владеет навыками работы с нормативными документами по определению требований о защите информации компьютерных систем.
Универсальные компетенции(УК)		
УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними, разрабатывает и содержательно аргументирует стратегию решения	Знать основы системного подхода. Уметь осуществлять критический анализ проблемных ситуаций на основе системного подхода. Владеть навыками выработки стратегий действий.
УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	Осуществляет критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.	Иметь опыт анализа проблемных ситуаций на основе системного подхода Уметь анализировать необходимую информацию в области информационной безопасности, содержащуюся в различных формах отчетности и прочих отечественных и зарубежных источника. Владеть навыками интерпретации информации, содержащейся в различных отечественных и зарубежных источниках в области информационной безопасности. Знать способы сбора и обработки данных, методологию и способы исследования в области информационной безопасности.

УК-2 Способен управлять проектом на всех этапах его жизненного цикла	Управлять проектом на создание СЗИ.	Иметь опыт построения систем управления проектами по разработке системы информационной безопасности информационных систем в условиях применения современных информационных технологий. Уметь моделировать риски. Владеть пониманием структуры и системы взаимосвязи процессов управления. Знать нормативные акты и стандарты в области управления проектами по разработке систем информационной безопасности.
УК-2 Способен управлять проектом на всех этапах его жизненного цикла	Разрабатывает концепцию проекта в рамках обозначенной проблемы: формулирует цель, задачи, обосновывает актуальность, значимость, ожидаемые результаты и возможные сферы их применения.	Знать особенности управления проектом на всех стадиях и этапах жизненного цикла. Уметь управлять проектом на всех этапах его жизненного цикла.
УК-2 Способен управлять проектом на всех этапах его жизненного цикла	Знает основные модели жизненного цикла проекта, его этапы и фазы, их характеристики и особенности.	Знает основы построения информационно-вычислительных систем; перечень конструкций и библиотек языков программирования, принципов построения программ в процедурно-ориентированной и объектно-ориентированной парадигмах. Умеет реализовывать алгоритмы на языке программирования, осуществлять работы с интегрированной средой разработки программного обеспечения, проводить оценку вычислительной сложности. Владеет навыками работы с интегрированной средой разработки программного обеспечения, определения вычислительной сложности реализуемых алгоритмов.
УК-3 Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	Организует работу персонала службы информационной безопасности по подготовке проекта организационно-распорядительной документации на системы защиты информации.	Иметь опыт организации обучения персонала использованию технических, программных (программно-технических) средств защиты информации. Уметь организовывать работу команды по подготовке проекта организационно-распорядительной документации на системы защиты информации. Владеть методами организации мер, обеспечивающих эффективность системы защиты информации. Знать основы трудового законодательства, требования ДИ работников службы информационной безопасности.
УК-3 Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	Планирует и корректирует работу команды с учетом интересов, особенностей поведения и мнений ее членов.	Знать основы работы в команде и порядок выработки командной стратегии для достижения поставленной цели. Уметь организовывать и руководить работой команды. Владеть навыками руководства работой команды и выработки командной стратегии для достижения поставленной цели.

УК-3 Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	Вырабатывает командную стратегию и организует работу команды для достижения целей	Знать особенности, основные методы и технологии разработки командной стратегии и организации командной работы. Уметь применять знания по выработке командной стратегии организации работы в команде. Владеть навыками организации и руководства работой команды.
УК-4 Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	Аргументированно и конструктивно отстаивает свои позиции и идеи в академических и профессиональных дискуссиях на государственном языке РФ и иностранном языке.	Знать правила коммуникативного поведения в ситуациях межкультурного научного и профессионального общения в устной и письменной формах. Уметь осуществлять устную коммуникацию в монологической и диалогической формах в ситуациях научного и профессионального обмена. Владеть терминологическим аппаратом по теме исследования, базовыми принципами структурирования и написания научных публикаций; навыком работы с международными базами научной информации.
УК-4 Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	Знает принципы построения устного и письменного высказывания на русском и иностранном(ых) языках, правила и закономерности деловой устной и письменной коммуникации; владеет широким словарным запасом, достаточным для осуществления деловой коммуникации в рамках академической и профессиональной направленности Составлять документы и научные тексты по результатам научного исследования в соответствии с требованиями, установленными нормами, особенностями стилей речи и стандартами. Применяет языковые нормы при составлении документов и научных текстов по исследованию безопасности объектов критической информационной инфраструктуры.
УК-5 Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	Выстраивает социальное профессиональное взаимодействие с учетом особенностей основных форм научного и религиозного сознания, деловой и общей культуры представителей других этносов и конфессий, различных социальных групп.	Знать основные проблемы философии науки и техники, а также современные подходы к их решению с учетом разнообразия культур; тенденции развития научных исследований и технических инноваций. Уметь использовать принципы научного познания при формировании собственной мировоззренческой позиции в условиях межкультурного взаимодействия; использовать понятия и категории философии в оценке этических проблем науки и техники. Владеть навыками философского анализа особенностей влияния научно-технического прогресса на культурные процессы в обществе; навыками толерантного общения в условиях многообразия социокультурных традиций и научно-теоретических установок.

УК-6 Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки	Определяет приоритеты профессионального роста и способы совершенствования собственной деятельности на основе самооценки по выбранным критериям.	Знать основы определения приоритетов и способы совершенствования собственной деятельности. Уметь определять и реализовывать приоритеты собственной деятельности. Владеть способностью совершенствовать собственную деятельность на основе самооценки.

1.6 Планируемые результаты обучения по каждой дисциплине (модулю) и практике - знания, умения, навыки и (или) опыт деятельности (индикаторы достижения компетенции), характерезующие этапы формирования компетенций и обеспечивающие достижение планируемых результатов освоения ОПОП

Планируемые результаты обучения по каждой дисциплине и практике – знания, умения, навыки и (или) опыт деятельности (индикаторы достижения компетенции), характеризующие этапы формирования компетенций и обеспечивающие достижение планируемых результатов освоения образовательной программы

Код и содержание компетенции	Индикаторы достижения компетенции	Результаты обучения
Государственная тайна и защита информации		
ПК-3 Владеет нормативно-методической базой обеспечения защиты сведений, составляющих государственную тайну	Владеет нормативной базой обеспечения области защиты государственной тайны, информационной безопасности, соблюдения режима секретности.	Знать требования правовых актов в области защиты государственной тайны и информационной безопасности, режима секретности Уметь соблюдать в профессиональной деятельности требования правовых актов в области защиты информации и сведений составляющих государственную тайну Владеть навыками обеспечения соблюдения режима секретности
Организация защиты объектов информатизации		
ПК-1 Владеет методикой проведения предпроектного обследования объектов информатизации и выделенных(защищаемых) помещений	Владеет методикой проведения предпроектного обследования объектов информатизации и выделенных(защищаемых) помещений	Знает содержание и порядок деятельности персонала объектов критической информационной инфраструктуры и ее частей. Знает нормативную базу, регламентирующую процессы обеспечения информационной безопасности объектов критической информационной инфраструктуры и ее частей. Умеет разрабатывать организационно-распорядительные документы по обеспечению безопасности значимых объектов критической информационной инфраструктуры. Владеет техническими мерами обеспечения безопасности значимых объектов критической информационной инфраструктуры.
ПК-2 Способен приводить аналитическое обоснование необходимости создания систем защиты информации	Способен приводить аналитическое обоснование необходимости создания систем защиты информации	Знает общие принципы организации защиты объектов критической информационной инфраструктуры и ее частей. Умеет организовывать защиту объектов критической информационной инфраструктуры и ее частей с учетом действующих нормативных и методических документов. Владеет методикой определения категории объектов критической информационной инфраструктуры.

ПК-4 Способен организовывать и сопровождать аттестацию объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации	Способен организовывать и сопровождать аттестацию объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации.	Знает нормативную базу, регламентирующую процессы аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации. Умеет разрабатывать организационно-распорядительные документы по сопровождению процессов аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации. Имеет опыт организации аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации.
Построение моделей угроз информационной безопасности		
ПК-6 Прогнозирует риски в информационной безопасности и управляет инцидентами информационной безопасности	Способен построить моделей угроз информационной безопасности, выявлять и оценивать актуальности угроз информационной безопасности, построения их моделей для определения требований о защите информации	Знает общую информацию об угрозах и нарушителях безопасности информации компьютерных систем. Знает методику выявления и оценки актуальности угроз информационной безопасности, построения их моделей для определения требований о защите информации Умеет выявлять и оценивать актуальности угроз информационной безопасности, построения их моделей для определения требований о защите информации Владеет навыками работы с нормативными документами по определению требований о защите информации компьютерных систем.
Ввод системы защиты информации в эксплуатацию		
ПК-5 Способен организовывать и проводить приемочные испытания СЗИ, вводить в эксплуатацию СЗИ	Способен организовывать и проводить приемочные испытания СЗИ, вводить в эксплуатацию СЗИ.	Нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации Уметь организовывать ввод системы защиты информации в эксплуатацию. Владеть навыками ввода системы защиты информации в эксплуатацию.
Организация приемочных испытаний системы защиты информации		
ПК-5 Способен организовывать и проводить приемочные испытания СЗИ, вводить в эксплуатацию СЗИ	Способен организовывать и проводить приемочные испытания СЗИ, вводить в эксплуатацию СЗИ	Нормативную базу регламентирующую приемочные испытания СЗИ при вводе в эксплуатацию СЗИ Умеет организовывать приемочные испытания системы защиты информации Методами организация приемочных испытаний системы защиты информации
Менеджмент профессиональной деятельности		
УК-3 Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	Планирует и корректирует работу команды с учетом интересов, особенностей поведения и мнений ее членов.	Знать основы работы в команде и порядок выработки командной стратегии для достижения поставленной цели. Уметь организовывать и руководить работой команды. Владеть навыками руководства работой команды и выработки командной стратегии для достижения поставленной цели.

УК-6 Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки	Определяет приоритеты профессионального роста и способы совершенствования собственной деятельности на основе самооценки по выбранным критериям.	Знать основы определения приоритетов и способы совершенствования собственной деятельности. Уметь определять и реализовывать приоритеты собственной деятельности. Владеть способностью совершенствовать собственную деятельность на основе самооценки.
Управление проектами		
УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними, разрабатывает и содержательно аргументирует стратегию решения	Знать основы системного подхода. Уметь осуществлять критический анализ проблемных ситуаций на основе системного подхода. Владеть навыками выработки стратегий действий.
УК-2 Способен управлять проектом на всех этапах его жизненного цикла	Разрабатывает концепцию проекта в рамках обозначенной проблемы: формулирует цель, задачи, обосновывает актуальность, значимость, ожидаемые результаты и возможные сферы их применения.	Знать особенности управления проектом на всех стадиях и этапах жизненного цикла. Уметь управлять проектом на всех этапах его жизненного цикла.
УК-3 Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	Вырабатывает командную стратегию и организует работу команды для достижения целей	Знать особенности, основные методы и технологии разработки командной стратегии и организации командной работы. Уметь применять знания по выработке командной стратегии организации работы в команде. Владеть навыками организации и руководства работой команды.
Иностранный язык в профессиональной деятельности		
УК-4 Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	Аргументированно и конструктивно отстаивает свои позиции и идеи в академических и профессиональных дискуссиях на государственном языке РФ и иностранном языке.	Знать правила коммуникативного поведения в ситуациях межкультурного научного и профессионального общения в устной и письменной формах. Уметь осуществлять устную коммуникацию в монологической и диалогической формах в ситуациях научного и профессионального обмена. Владеть терминологическим аппаратом по теме исследования, базовыми принципами структурирования и написания научных публикаций; навыком работы с международными базами научной информации.
Философские проблемы науки и техники		
УК-5 Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	Выстраивает социальное профессиональное взаимодействие с учетом особенностей основных форм научного и религиозного сознания, деловой и общей культуры представителей других этносов и конфессий, различных социальных групп.	Знать основные проблемы философии науки и техники, а также современные подходы к их решению с учетом разнообразия культур; тенденции развития научных исследований и технических инноваций. Уметь использовать принципы научного познания при формировании собственной мировоззренческой позиции в условиях межкультурного взаимодействия; использовать понятия и категории философии в оценке этических проблем науки и техники. Владеть навыками философского анализа особенностей влияния научно-технического прогресса на культурные процессы в обществе; навыками толерантного общения в условиях многообразия социокультурных традиций и научно-теоретических установок.
Защищенные информационные системы		

ОПК-1 Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;	Обосновывает требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание.	Знает принципы разработки защищенных информационных систем различного применения и степени сложности. Знает методики выявления угроз и оценки уязвимостей информационных систем. Знает методы и средства обеспечения информационной безопасности, а также нормативную базу регламентирующую классификацию данных средств. Знает типовые требования к разработке средств защиты, направленные на снижение рисков информационной безопасности. Умеет обосновывать требования к процессам и технологиям обеспечения информационной безопасности объектов критической информационной инфраструктуры. Умеет осуществлять выбор подсистем, реализующих технологии обеспечения информационной безопасности для объектов критической информационной инфраструктуры. Умеет обосновывать требования к мерам обеспечения информационной безопасности объектов критической информационной инфраструктуры. Умеет составлять техническое задание по разработке систем, комплексов, средств и технологий обеспечения информационной безопасности. Умеет настраивать средства защиты информации в соответствии с требованиями к объекту защиты с целью снижения рисков информационной безопасности Владеть навыками разработки комплексной инфраструктуры защищенной информационной системы, навыками разработки проектов нормативных и правовых актов предприятия, учреждения, организации, регламентирующих деятельность по обеспечению ИБ.

ОПК-2 Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности;	Разрабатывает технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности.	Знает принципы организации и этапы разработки системы (подсистемы либо компонента системы) обеспечения информационной безопасности объектов критической информационной инфраструктуры. Знает методики испытаний средств и систем обеспечения информационной безопасности. Умеет составлять требования и критерии оценки информационной безопасности. Умеет разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности объектов критической информационной инфраструктуры. Умеет разрабатывать требования к средствам и методам контроля проектируемой системы (подсистемы либо компонента системы) обеспечения информационной безопасности объектов критической информационной инфраструктуры. Умеет разрабатывать и реализовывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности объектов критической информационной инфраструктуры. Владеть навыками технических проектов систем (подсистемы либо компонента системы) обеспечения информационной безопасности.
Управление информационной безопасностью		

ОПК-1 Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;	Обосновывает требования к системе обеспечения информационной безопасности и разрабатывает проекты технического задания на ее создание.	Знать основные принципы организации технического, программного и информационною обеспечения защищенных информационных систем; основные механизмы информационной безопасности и типовые процессы управления этими механизмами в информационной системе; основные угрозы безопасности информации и модели нарушителя в информационных системах; принципы формирования политики информационной безопасности в информационных системах; методы аттестации уровня защищенности информационных систем; основные методы управления информационной безопасностью; основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем. Уметь строить системы обеспечения информационной безопасности в различных условиях функционирования защищаемых информационных систем; разрабатывать модели угроз и нарушителей информационной безопасности информационных систем; разрабатывать частные политики информационной безопасности информационных систем; контролировать эффективность принятых мер по реализации частных политик информационной безопасности информационных систем; оценивать информационные риски в информационных системах; разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных систем; составлять аналитические обзоры по вопросам обеспечения информационной безопасности информационных систем; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности. Владеть методами и средствами выявления угроз безопасности информационным системам; навыками выбора и обоснования критериев эффективности функционирования защищенных информационных систем; навыками участия в экспертизе состояния защищенности информации на объекте защиты; методами управления информационной безопасностью информационных систем; методами опенки информационных рисков; методами организации и управления деятельностью служб защиты информации на предприятии; навыками управления информационной безопасностью простых объектов.



ОПК-3 Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности;	Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности	Знает нормативную и правовую базу в области управления информационной безопасностью объектов критической информационной инфраструктуры. Знает отечественные и зарубежные стандарты в области управления информационной безопасностью объектов критической информационной инфраструктуры. Знает структуру политик обеспечения информационной безопасности объектов критической информационной инфраструктуры и требования к их содержанию Умеет разрабатывать проекты нормативных и организационно-распорядительных документов по обеспечению информационной безопасности объектов критической информационной инфраструктуры. Умеет разрабатывать политику информационной безопасности объектов критической информационной инфраструктуры различных уровней Владеет навыками разработки политики информационной безопасности различных уровней
Основы научных исследований		
ОПК-4 Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок;	Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок	Знает основные формы, методы и приемы научного исследования области безопасности объектов критической информационной инфраструктуры. Умеет составлять план научного исследования в области безопасности объектов критической информационной инфраструктуры и проводить деятельность в соответствии с составленным планом. Умеет разрабатывать программу разработки компонентов средств защиты информации для объектов критической информационной инфраструктуры. Демонстрирует способности анализа наборов данных при помощи различных сред их анализа с наглядной визуализацией получаемых результатов
ОПК-5 Способен проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи.	Способен проводить научные исследования.	Знать методы научных исследований; организацию научных исследований и этапы их проведения; процедуры разработки и проектирования новых технических объектов; теоретические исследования; построение моделей физических процессов и объектов; проведение экспериментальных исследования и обработка их результатов. Уметь применять методы научных исследований ; организовывать научные исследования; проводить экспериментальные исследования и обрабатывать их результаты. Владеть методами научных исследований ; организации научных исследований; навыками экспериментальных исследований и обработки их результатов.

УК-4 Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	Знает принципы построения устного и письменного высказывания на русском и иностранном(ых) языках, правила и закономерности деловой устной и письменной коммуникации; владеет широким словарным запасом, достаточным для осуществления деловой коммуникации в рамках академической и профессиональной направленности Составлять документы и научные тексты по результатам научного исследования в соответствии с требованиями, установленными нормами, особенностями стилей речи и стандартами. Применяет языковые нормы при составлении документов и научных текстов по исследованию безопасности объектов критической информационной инфраструктуры.
Организационно-распорядительная документация по обеспечению информационной безопасности		
ОПК-3 Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности;	Разрабатывает проекты организационно-распорядительных документов по обеспечению информационной безопасности.	Знать источники правовой информации, виды нормативных правовых актов, стандарты в области информационной безопасности. Уметь анализировать, изучать и обобщать правовую информацию, определять релевантные для профессиональной деятельности нормативные акты, использовать нормативные и методические документы при оформлении технической документации. Владеть навыками обоснования своих решений на основе действующего законодательства, навыками поиска требуемой информации используя нормативные правовые акты, навыками подготовки проектов организационно-распорядительных документов по обеспечению информационной безопасности.
Проектирование систем (компонента системы) обеспечения информационной безопасности		

ОПК-2 Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности;	Разрабатывает технический проект системы обеспечения информационной безопасности, а также их компонент(подсистемы).	Знать основные принципы разработки политики информационной безопасности на предприятии, принципы анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности, современную аппаратно-программную базу компьютерной техники для решения задач защиты информации. Уметь применять комплексный подход к обеспечению информационной безопасности объекта защиты, проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности, применять программные средства системного, прикладного и средства системного, специального назначения, инструментальные средства, языки и системы программирования для решения задач защиты информации. Владеть основными методами обеспечения информационной безопасности объекта защиты, методами технико-экономического обоснования проектных решений, методами и средствами системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения задач защиты информации.
Информационная безопасность интернета вещей		

ОПК-2 Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности;	Разрабатывает требования к средствам и методам контроля проектируемой системы (подсистемы либо компонента системы) обеспечения информационной безопасности.	Знает принципы построения систем на базе IoTустройств, а также способы их эффективной реализации; существующие технологии в области Интернета вещей; стандарты реализации интерфейсов подключаемых устройств; стандарты информационного взаимодействия систем. Знает типовые средства и методы защиты информации в локальных и глобальных вычислительных сетях; требования НПА и стандартов по разработке моделей угроз информационной безопасности; наиболее распространенные уязвимости IoTустройств и протоколов передачи данных; средства обеспечения информационной безопасности IoT-систем; принципы построения защищенных телекоммуникационных систем; механизмы реализации атак в сетях Интернета вещей; Умеет проводить анализ защищенности IoT-систем; Разрабатывать модели угроз для систем Интернета Вещей. Умеет проводить первичную настройку и проверку функционирования СССЭ, средств и систем защиты СССЭ от НСД; разбираться в существующих IoT-технологиях и применять их к конкретным сценариям; внедрять типовые решения по информационной безопасности IoT-систем; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты в соответствии с требованиями нормативно правовых актов и нормативных методических документов. Владеет способами конфигурировать параметры системы защиты информации автоматизированной системы в соответствии с ее эксплуатационной документацией; работать с документацией прилагаемой разработчиком устройства; обнаруживать типовые уязвимости IoT систем. Может формировать требования и разрабатывать спецификации для проектируемой системы на базе IoTустройств; планировать разработку сложных системы на базе IoT-устройств; проводить выбор эффективных способов реализации структур системы на базе IoTустройств при решении профессиональных задач.
Технологии обеспечения информационной безопасности		

ОПК-1 Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;	Способен обосновывать требования к системе обеспечения информационной безопасности .	Знает технологии обеспечения информационной безопасности. Знает основные виды уязвимостей систем и угрозы информационной безопасности. Знает методы и средства обеспечения информационной безопасности, а также нормативную базу регламентирующую классификацию данных средств. Умеет обосновывать выбор средств защиты информации для противодействия конкретным угрозам. Умеет осуществлять подбор средств защиты информации в соответствии с заданными критериями. Умеет обосновывать требования к мерам обеспечения информационной безопасности в соответствии с нормативной базой. Умеет составлять техническое задание по обеспечению информационной безопасности на объекте с использованием сертифицированных ФСТЭК средств защиты информации. Владеет опытом настройки средства защиты информации в соответствии с требованиями к объекту защиты с целью снижения рисков информационной безопасности.
ОПК-2 Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности;	Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности .	Знает принципы эксплуатации средств защиты информации. Знает методы тестирования средств защиты информационной безопасности. Умеет осуществлять настройку режимов работы средств защиты информации в соответствии с определенными моделями угроз. Умеет разрабатывать сценарии тестирования средств защиты информации. Умеет разрабатывать требования к средствам защиты информации. Умеет управлять средствами защиты информации в соответствии с требованиями к объекту защиты. Имеет опыт разработки требования к средствам и методам контроля проектируемой системы (подсистемы либо компонента системы) обеспечения информационной безопасности.
Практика производственная, организационно-управленческая практика		
ПК-3 Владеет нормативно-методической базой обеспечения защиты сведений, составляющих государственную тайну	Владеет нормативно-методической базой обеспечения защиты сведений, составляющих государственную тайну.	Знать нормативную базу для обеспечения защиты сведений, составляющих государственную тайну. Уметь использовать полученные знания в профессиональной деятельности. Владеть нормативно-методической базой обеспечения защиты сведений, составляющих государственную тайну. Иметь опыт подготовки нормативно-методической базы.

ПК-4 Способен организовывать и сопровождать аттестацию объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации	Организует и сопровождает аттестацию объектов вычислительной техники и выделенных защищаемых помещений на соответствие требованиям по защите информации.	Знать порядок аттестации объектов информатизации на соответствие требованиям по защите информации. Уметь подготавливать объекты вычислительной техники и выделенные (защищаемые) помещения к аттестации по требованиям безопасности информации. Владеть методами подготовки объектов вычислительной техники и выделенных (защищаемых) помещений к аттестации. Иметь опыт организации подготовки объектов вычислительной техники и выделенных (защищаемых) помещений к аттестации по требованиям безопасности информации.
ПК-5 Способен организовывать и проводить приемочные испытания СЗИ, вводить в эксплуатацию СЗИ	Организует и проводит приемочные испытания СЗИ, вводит в эксплуатацию СЗИ.	Знать методы защиты информации от утечки, эксплуатационную документацию на систему защиты информации. Уметь организовывать приемочные испытания системы защиты информации Владеть способами приемочных испытаний СЗИ, ввода в эксплуатацию СЗИ. Иметь опыт организации приемочных испытаний систем защиты информации.
ПК-6 Прогнозирует риски в информационной безопасности и управляет инцидентами информационной безопасности	Прогнозирует риски в информационной безопасности и управляет инцидентами информационной безопасности.	Знать количественный и качественный подходы к оценке рисков ИБ. Уметь проводить качественную оценку рисков, определять вероятность реализации угрозы по отношению к информационному активу, определять уровень возможности успешной реализации угрозы с учетом текущего состояния ИБ, внедренных мер и средств защиты. Владеть методами разработки мер безопасности, контрмер и действий по каждой актуальной угрозе для снижения уровня риска, управлять инцидентами информационной безопасности. Иметь опыт определения риски в информационной безопасности и управления инцидентами информационной безопасности.
УК-2 Способен управлять проектом на всех этапах его жизненного цикла	Управлять проектом на создание СЗИ.	Знать нормативные акты и стандарты в области управления проектами по разработке систем информационной безопасности. Уметь моделировать риски. Владеть пониманием структуры и системы взаимосвязи процессов управления. Иметь опыт построения систем управления проектами по разработке системы информационной безопасности информационных систем в условиях применения современных информационных технологий.

УК-3 Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	Организует работу персонала службы информационной безопасности по подготовке проекта организационно-распорядительной документации на системы защиты информации.	Знать основы трудового законодательства, требования ДИ работников службы информационной безопасности. Уметь организовывать работу команды по подготовке проекта организационно-распорядительной документации на системы защиты информации. Владеть методами организации мер, обеспечивающих эффективность системы защиты информации. Иметь опыт организации обучения персонала использованию технических, программных (программно-технических) средств защиты информации.
Практика производственная, преддипломная практика		
ПК-1 Владеет методикой проведения предпроектного обследования объектов информатизации и выделенных(защищаемых) помещений	Владеет методикой проведения предпроектного обследования объектов информатизации и выделенных защищаемых помещений.	Знать методологию проектирования систем, комплексов, средств и технологий обеспечения информационной безопасности, необходимые для разработки систем, комплексов, средств и технологий обеспечения информационной безопасности. Уметь выполнять проектирование и разработку систем, комплексов, средств и технологий обеспечения информационной безопасности. Владеть навыками работы в среде CASE-средств анализа и проектирования систем навыками использования в практической деятельности новых знаний и умений. Иметь опыт проведения предпроектного обследования объектов информатизации и выделенных защищаемых помещений.
ПК-2 Способен приводить аналитическое обоснование необходимости создания систем защиты информации	Приводит аналитическое обоснование необходимости создания систем защиты информации.	Знать российские и международные стандарты в области информационной безопасности. Уметь проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты. Владеть навыками обеспечения информационной безопасностью объектов защиты. Иметь опыт приведения аналитическое обоснование необходимости создания систем защиты информации.
ПК-3 Владеет нормативно-методической базой обеспечения защиты сведений, составляющих государственную тайну	Владеет нормативно-методической базой обеспечения защиты сведений, составляющих государственную тайну.	Знать основные принципы организации систем, средств и технологий обеспечения информационной безопасности. Уметь организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами. Владеть знаниями законодательных и правовых актов в области безопасности; правилами составления локальных нормативных актов и регламентов в области информационной безопасности. Иметь опыт подготовки нормативно-методической базы по защите сведений, составляющих государственную тайну.

ПК-4 Способен организовывать и сопровождать аттестацию объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации	Организует и сопровождает аттестацию объектов вычислительной техники и выделенных защищаемых помещений на соответствие требованиям по защите информации.	Знать понятия контура безопасности, физические и математические методы исследования защищенности объектов; порядок проведения аттестации объектов информатизации по требованиям безопасности информации, требования стандартов и иных нормативно-технических документов по безопасности информации, утвержденных Гостехкомиссией России. Уметь проводить экспериментальные исследования защищенности объектов, разрабатывать требования к защите от утечек по техническим каналам. Владеть методами инструментального контроля защищенности объекта. Иметь опыт организации и сопровождения аттестации объектов вычислительной техники и выделенных защищаемых помещений на соответствие требованиям по защите информации.
ПК-5 Способен организовывать и проводить приемочные испытания СЗИ, вводить в эксплуатацию СЗИ	Организует и проводит приемочные испытания СЗИ, вводит в эксплуатацию СЗИ.	Знать методы защиты информации от утечки, эксплуатационную документацию на систему защиты информации. Уметь организовывать приемочные испытания системы защиты информации. Владеть способами приемочных испытаний СЗИ, ввода в эксплуатацию СЗИ. Иметь опыт организации приемочных испытаний систем защиты информации.
ПК-6 Прогнозирует риски в информационной безопасности и управляет инцидентами информационной безопасности	Прогнозирует риски в информационной безопасности и управляет инцидентами информационной безопасности.	Знать порядок организации деятельности по управлению информационной безопасностью. Уметь организовать процесс управления информационной безопасностью. Владеть навыками управления системой информационной безопасности. Иметь опыт анализа рисков в информационной безопасности и управлении инцидентами информационной безопасности.
УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	Осуществляет критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.	Знать способы сбора и обработки данных, методологию и способы исследования в области информационной безопасности. Уметь анализировать необходимую информацию в области информационной безопасности, содержащуюся в различных формах отчетности и прочих отечественных и зарубежных источника. Владеть навыками интерпретации информации, содержащейся в различных отечественных и зарубежных источниках в области информационной безопасности. Иметь опыт анализа проблемных ситуаций на основе системного подхода
Практика производственная, проектно-технологическая практика		

ОПК-1 Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;	Обосновывает требования к системе обеспечения информационной безопасности и способен разработать проект технического задания на ее создание.	Знать уязвимости информационных ресурсов, возможные угрозы безопасности информации, информационные процессы объектов. Уметь определять информационные ресурсы, подлежащие защите информации, угрозы безопасности информации. Владеть профессиональной терминологией в области обеспечения безопасности персональных данных; методами мониторинга и аудита, выявления угроз и управления информационной безопасностью. Иметь опыт формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем.
ОПК-2 Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности;	Способен разработать технические проекты систем (подсистем) либо компонента системы обеспечения информационной безопасности.	Знать основы организации защиты государственной тайны и конфиденциальной информации; методы анализа информационной безопасности объектов и систем; стандарты в области информационной безопасности. Уметь отечественные и зарубежные стандарты в области компьютерной безопасности и информационной безопасности объектов для проектирования, разработки и оценки защищенности компьютерных систем. Владеть методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов. Иметь опыт разработки технических проектов систем (подсистем) либо компонента системы обеспечения информационной безопасности.
ОПК-3 Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности;	Способен разработать проекты организационно-распорядительных документов по обеспечению информационной безопасности.	Знать требования основных действующих государственных стандартов (ГОСТ) регламентирующие построение, проектирование и эксплуатацию информационных и аналитических систем. Уметь осуществлять подготовку технических заданий на построение и проектирование информационных и аналитических систем; осуществлять подготовку организационно-распорядительной документации (инструкции, приказы, распоряжения) регламентирующей эксплуатацию информационных систем. Владеть навыками оформления рабочей технической документации. Иметь опыт разработки проектов организационно-распорядительных документов по обеспечению информационной безопасности.

ОПК-4 Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок;	Осуществляет сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок.	Знать методы проектирования автоматизированных систем; основные принципы проектного управления. Уметь проектировать и сопровождать типовые специализированные автоматизированные информационные системы, локальные сети; осуществлять подготовку технико-экономических обоснований соответствующих проектных решений. Владеть навыками определения затрат компании на информационную безопасность и проведения зависимости между затратами и уровнем защищенности. Иметь опыт сбора, обработки и анализа научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок.
ОПК-5 Способен проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи.	Проводит научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи.	Знать основные принципы экспериментальных исследований, соотношение теоретического и экспериментального знания, методику проведения экспериментов. Уметь разбираться в лабораторном оборудовании по профилю своей деятельности и работать с оборудованием для проведения экспериментов, применять методики, обрабатывать результаты, проводить оценку погрешности, проводить экспериментально-исследовательские работы системы защиты информации. Владеть навыками выполнения расчетов, обработки результатов экспериментов, оценки погрешностей и достоверности результатов, навыками проведения экспериментально-исследовательских работ системы защиты информации. Иметь опыт оформления научно-технических отчетов, обзоров, результатов выполненных исследований, научных докладов и статей.
Сертификация средств защиты информации		
ПК-3 Владеет нормативно-методической базой обеспечения защиты сведений, составляющих государственную тайну	Владеет нормативно-методической базой обеспечения защиты сведений, составляющих государственную тайну.	Знать нормативно-правовое обеспечение сертификации технических и программных средств защиты информации, правила лицензирования и сертификации в области защиты информации; порядок проведения аттестации объектов информационной защиты. Уметь применять стандарты и другие нормативные документы при оценке, контроле качества и сертификации; определять рациональные способы и средства защиты информации на объекте информатизации; организовать мероприятия по защите информации на объекте информатизации. Владеть схемами сертификации и правилами декларирования соответствия; признаками обязательной и добровольной сертификации.
Искусственный интеллект		

УК-2 Способен управлять проектом на всех этапах его жизненного цикла	Знает основные модели жизненного цикла проекта, его этапы и фазы, их характеристики и особенности.	Знает основы построения информационно-вычислительных систем; перечень конструкций и библиотек языков программирования, принципов построения программ в процедурно-ориентированной и объектно-ориентированной парадигмах. Умеет реализовывать алгоритмы на языке программирования, осуществлять работы с интегрированной средой разработки программного обеспечения, проводить оценку вычислительной сложности. Владеет навыками работы с интегрированной средой разработки программного обеспечения, определения вычислительной сложности реализуемых алгоритмов.

1.7 Сведения о профессорско-преподавательском составе, необходимом для реализации образовательной программы

1. Реализация программы магистратуры обеспечивается педагогическими работниками Организации, а также лицами, привлекаемыми Организацией к реализации программы магистратуры на иных условиях.
2. Квалификация педагогических работников Организации отвечает квалификационным требованиям, указанным в квалификационных справочниках и (или) профессиональных стандартах (при наличии).
3. Не менее 80 процентов численности педагогических работников Организации, участвующих в реализации программы магистратуры, и лиц, привлекаемых Организацией к реализации программы магистратуры на иных условиях (исходя из количества замещаемых ставок, приведенного к целочисленным значениям), ведут научную, учебно-методическую и (или) практическую работу, соответствующую профилю преподаваемой дисциплины (модуля).
4. Не менее 5 процентов численности педагогических работников Организации, участвующих в реализации программы магистратуры, и лиц, привлекаемых Организацией к реализации программы магистратуры 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 (иметь стаж работы в данной профессиональной сфере не менее 3 лет).
5. Доля педагогических работников Организации (исходя из количества замещаемых ставок, приведенного к целочисленным значениям) составляет не менее 55 процентов от общего количества лиц, привлекаемых к реализации программы магистратуры.
6. Не менее 60 процентов численности педагогических работников Организации и лиц, привлекаемых к образовательной деятельности Организации на иных условиях (исходя из количества замещаемых ставок, приведенного к целочисленным значениям), 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 программы магистратуры должен принимает участие 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".

1. Общее руководство научным содержанием программы магистратуры осуществляется научно-педагогическим работником Организации, имеющим ученую степень (в том числе ученую степень, полученную в иностранном государстве и признаваемую в Российской Федерации), осуществляющим самостоятельные научно-исследовательские (творческие) проекты (участвующим в осуществлении таких проектов) по направлению подготовки, имеющим ежегодные публикации по результатам

указанной научно-исследовательской (творческой) деятельности в ведущих отечественных рецензируемых научных журналах и изданиях, а также осуществляющим ежегодную апробацию результатов указанной научно- исследовательской (творческой) деятельности на национальных и международных конференциях.

2. Иные сведения

Образовательная деятельность по образовательной программе проводится:

- в форме контактной работы обучающихся с НПР (далее – контактная работа);
- в форме самостоятельной работы обучающихся;
- в иных формах, определяемых рабочими программам дисциплин (модулей), программами практик.

Контактная работа может быть аудиторной, внеаудиторной, а также проводиться в электронной информационно-образовательной среде КузГТУ – Автоматизированной Информационной Системе (АИС) «Портал. КузГТУ».

Учебные занятия по дисциплинам (модулям), промежуточная аттестация обучающихся и итоговая (государственная итоговая) аттестация обучающихся проводятся в форме контактной работы и в форме самостоятельной работы обучающихся.

Контактная работа при проведении учебных занятий по дисциплинам (модулям) включает в себя:

- занятия лекционного типа (лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации НПР обучающимся);
- занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия);
- групповые консультации;
- индивидуальную работу обучающихся с НПР (в том числе индивидуальные консультации);
- иную контактную работу (при необходимости), предусматривающую групповую или индивидуальную работу обучающихся с НПР.

Практика проводится в форме контактной работы и в иных формах, установленных программой практики.

2.1 Перечень методов, средств обучения и образовательных технологий

№ п/п	Наименование образовательной технологии	Краткая характеристика
1	Кейс-технологии	Технология, основанная на комплектовании наборов (кейсов) материалов по теме и заданий по проблемной ситуации в ней, и передачи их обучающимся для самостоятельного изучения и решения с последующим коллективным обсуждением вариантов для выработки наиболее рациональных предложений
2	Технология деловой игры	Технология, основанная на комплектовании наборов (кейсов) материалов по теме и заданий по проблемной ситуации в ней, и передачи их обучающимся для самостоятельного изучения и решения с последующим коллективным обсуждением вариантов для выработки наиболее рациональных предложений
3	Информационные технологии	Использование актуальных ИТ и программных средств, востребованных в соответствующих отраслях для решения профессиональных задач
4	Сквозные цифровые технологии	Применение обучающимися цифровых технологий (как сквозных, так и новых производственных), востребованных в отрасли, для решении задач профессиональной деятельности
5	Технологии проблемного обучения	Решение обучающимися поставленных проблемных задач и проблемных ситуаций, требующих самостоятельного поиска дополнительных знаний и способов нахождения неизвестного
6	Технологии проектного обучения	Специально организованная учебная деятельность обучающихся, ограниченная во времени, нацеленная на решение определенной проблемы и имеющая в качестве результата конечный продукт деятельности – проект.
7	Технологии искусственного интеллекта	Применение обучающимися элементов искусственного интеллекта для решении задач профессиональной деятельности

8	Практико – ориентированные технологии	Выполнение обучающимися определенных видов работ, связанных с будущей профессиональной деятельностью и направленных на формирование, закрепление, развитие практических навыков и компетенций по профилю соответствующей образовательной программы при реализации дисциплин (модулей), практики, иных компонентов образовательных программ, предусмотренных учебным планом
9	Электронное обучение, дистанционные образовательные технологии	Организация учебных занятий в виде онлайн-курсов, обеспечивающих для обучающихся независимо от их места нахождения и места нахождения КузГТУ, достижение и оценку результатов обучения путем организации образовательной деятельности в электронной информационно-образовательной среде КузГТУ, к которой предоставляется открытый доступ через информационно-телекоммуникационную сеть "Интернет"

2.2 Нормативные документы для разработки образовательной программы

– Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;

– Приказ Минобрнауки России от 6 апреля 2021 г. № 245 «Об утверждении порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры»;

- Приказ Минобрнауки РФ от 26 ноября 2020 г. № 1455 «Об утверждении федерального государственного образовательного стандарта высшего образования - магистратура направлению подготовки 10.04.01 Информационная безопасность.

– Профессиональные стандарты;

– Устав КузГТУ.

2.3 Требования к материально-техническому и учебно-методическому обеспечению образовательной программы

Для изучения дисциплин может использоваться следующее программное обеспечение:

1. 7-zip
2. Open Office
3. Microsoft Windows
4. ESET NOD32 Smart Security Business Edition
5. Kaspersky Endpoint Security
6. Браузер Спутник
7. Libre Office
8. Mozilla Firefox
9. Google Chrome
10. Opera
11. Yandex
12. Microsoft Project
13. GIMP

2.4 Особенности организации образовательной деятельности для обучающихся с ограниченными возможностями здоровья

2.4.1. Для обеспечения образования инвалидов и обучающихся с ограниченными возможностями здоровья (далее вместе – обучающиеся с ОВЗ) в КузГТУ созданы специальные условия обучения (воспитания), в том числе специальные образовательные программы и методы обучения, индивидуальные технические средства обучения и среда жизнедеятельности, а также предоставляются педагогические, медицинские, социальные и иные услуги, без которых лицам с ОВЗ невозможно (затруднено) освоение образовательных программ.

Обучающимся с ОВЗ обеспечена беспрепятственная доступность прилегающей к КузГТУ территории, входных путей, путей перемещения внутри здания, территория КузГТУ соответствует условиям беспрепятственного, безопасного и удобного передвижения лиц, указанной категории. Выбор мест прохождения практики для обучающихся с ОВЗ осуществляется с учетом требований их доступности, рекомендаций медико-социальной экспертизы относительно условий и видов труда, содержащихся в индивидуальной программе реабилитации инвалида.

Обучающиеся с ОВЗ могут обучаться по индивидуальному учебному плану и адаптированной образовательной программе с учетом их особенностей и образовательных потребностей. При

необходимости возможно увеличение срока обучения на срок, установленный в соответствии с ФГОС для указанной категории лиц. При составлении индивидуального учебного плана и адаптированной образовательной программы могут предусматриваться различные варианты проведения занятий. С целью комплексного сопровождения обучающихся с ОВЗ привлекаются специалисты, имеющие соответствующую квалификацию.

2.4.2. Адаптированная образовательная программа разрабатывается с учетом индивидуальных программам реабилитации, абилитации исходя из конкретной ситуации и индивидуальных потребностей обучающегося с ОВЗ.

Образовательный процесс осуществляется с использованием специальной аппаратуры, мультимедийных и иных технических средств передачи и приема учебной информации, обеспечивается печатными и (или) электронными образовательными ресурсами в формах, адаптированных к ограничениям здоровья.

В адаптированной образовательной программе предусматриваются адаптационные дисциплины (в составе вариативной части), устанавливается особый порядок освоения дисциплин (модулей) по физической культуре и спорту, определяются методы обучения, формы проведения текущего контроля успеваемости, промежуточной и итоговой (государственной итоговой) аттестации с учетом состояния здоровья, доступности и индивидуальных психофизических особенностей обучающегося с ОВЗ.

2.5 Государственная итоговая аттестация

В состав Государственной итоговой аттестации входит: подготовка к процедуре защиты и защита выпускной квалификационной работы .

Государственный экзамен: не предусмотрен.

3. Рабочая программа воспитания и календарный план воспитательной работы

https://portal.kuzstu.ru/assets/docs/work_program_of_education.pdf
https://portal.kuzstu.ru/assets/docs/educational_work_schedule.pdf

4. Внесение изменений

№ изменения	Дата внесения изменения	Номера листов	Шифр документа	Краткое содержание изменения, отметка о ревизии	ФИО, подпись
1	2	3	4	5	6