

МИНОБРНАУКИ РОССИИ

федеральное государственное бюджетное образовательное учреждение
высшего образования

«Кузбасский государственный технический университет имени Т. Ф. Горбачева»

Аннотация к рабочей программе дисциплины

Ввод системы защиты информации в эксплуатацию

Направление подготовки «10.04.01 Информационная безопасность»
Направленность (профиль) подготовки «01 Организация и технология защиты информации»

Присваиваемая квалификация
"Магистр"

Формы обучения
очная

Кемерово 2025 г.

1. Перечень планируемых результатов обучения по дисциплине "Ввод системы защиты информации в эксплуатацию", соотнесенных с планируемыми результатами освоения образовательной программы

Освоение дисциплины направлено на формирование:
профессиональных компетенций:

ПК-5 - Способен организовывать и проводить приемочные испытания СЗИ, вводить в эксплуатацию СЗИ

Знать: Нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации

Уметь: Уметь организовывать ввод системы защиты информации в эксплуатацию.

Владеть: Владеть навыками ввода системы защиты информации в эксплуатацию.

В результате освоения дисциплины обучающийся в общем по дисциплине должен

Знать:

- Нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации

Уметь:

- Уметь организовывать ввод системы защиты информации в эксплуатацию.

Владеть:

- Владеть навыками ввода системы защиты информации в эксплуатацию.

2. Место дисциплины "Ввод системы защиты информации в эксплуатацию" в структуре ОПОП магистратуры

Для освоения дисциплины необходимы компетенции (знания умения, навыки и (или) опыт профессиональной деятельности), сформированные в рамках изучения следующих дисциплин: Защищенные информационные системы, Организационно-распорядительная документация по обеспечению информационной безопасности, Сертификация средств защиты информации.

Дисциплина входит в Блок 1 «Дисциплины (модули)» ОПОП. Цель дисциплины - получение обучающимися знаний, умений, навыков и (или) опыта профессиональной деятельности, необходимых для формирования компетенций, указанных в пункте 1.

МИНОБРНАУКИ РОССИИ

федеральное государственное бюджетное образовательное учреждение
высшего образования

«Кузбасский государственный технический университет имени Т. Ф. Горбачева»

Аннотация к рабочей программе дисциплины

Иностранный язык в профессиональной деятельности

Направление подготовки «10.04.01 Информационная безопасность»
Направленность (профиль) подготовки «01 Организация и технология защиты информации»

Присваиваемая квалификация
"Магистр"

Формы обучения
очная

Кемерово 2025 г.

1. Перечень планируемых результатов обучения по дисциплине "Иностранный язык в профессиональной деятельности", соотнесенных с планируемыми результатами освоения образовательной программы

Освоение дисциплины направлено на формирование:
универсальных компетенций:

УК-4 - Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия

Знать: Знать правила коммуникативного поведения в ситуациях межкультурного научного и профессионального общения в устной и письменной формах.

Уметь: Уметь осуществлять устную коммуникацию в монологической и диалогической формах в ситуациях научного и профессионального обмена.

Владеть: Владеть терминологическим аппаратом по теме исследования, базовыми принципами структурирования и написания научных публикаций; навыком работы с международными базами научной информации.

В результате освоения дисциплины обучающийся в общем по дисциплине должен

Знать:

- Знать правила коммуникативного поведения в ситуациях межкультурного научного и профессионального общения в устной и письменной формах.

Уметь:

- Уметь осуществлять устную коммуникацию в монологической и диалогической формах в ситуациях научного и профессионального обмена.

Владеть:

- Владеть терминологическим аппаратом по теме исследования, базовыми принципами структурирования и написания научных публикаций; навыком работы с международными базами научной информации.

2. Место дисциплины "Иностранный язык в профессиональной деятельности" в структуре ОПОП магистратуры

Для освоения дисциплины необходимы компетенции (знания умения, навыки и (или) опыт профессиональной деятельности), сформированные в рамках изучения следующих дисциплин: .

Дисциплина входит в Блок 1 «Дисциплины (модули)» ОПОП. Цель дисциплины - получение обучающимися знаний, умений, навыков и (или) опыта профессиональной деятельности, необходимых для формирования компетенций, указанных в пункте 1.

МИНОБРНАУКИ РОССИИ

федеральное государственное бюджетное образовательное учреждение
высшего образования

«Кузбасский государственный технический университет имени Т. Ф. Горбачева»

Аннотация к рабочей программе дисциплины

Управление проектами

Направление подготовки «10.04.01 Информационная безопасность»
Направленность (профиль) подготовки «01 Организация и технология защиты информации»

Присваиваемая квалификация
"Магистр"

Формы обучения
очная

Кемерово 2025 г.

1. Перечень планируемых результатов обучения по дисциплине "Управление проектами", соотнесенных с планируемыми результатами освоения образовательной программы

Освоение дисциплины направлено на формирование:
универсальных компетенций:

УК-1 - Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий

Знать: Знать основы системного подхода.

Уметь: Уметь осуществлять критический анализ проблемных ситуаций на основе системного подхода.

Владеть: Владеть навыками выработки стратегий действий.

УК-2 - Способен управлять проектом на всех этапах его жизненного цикла

Знать: Знать особенности управления проектом на всех стадиях и этапах жизненного цикла.

Уметь: Уметь управлять проектом на всех этапах его жизненного цикла.

Владеть:

УК-3 - Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели

Знать: Знать особенности, основные методы и технологии разработки командной стратегии и организации командной работы.

Уметь: Уметь применять знания по выработке командной стратегии организации работы в команде.

Владеть: Владеть навыками организации и руководства работой команды.

В результате освоения дисциплины обучающийся в общем по дисциплине должен

Знать:

- Знать основы системного подхода.

- Знать особенности управления проектом на всех стадиях и этапах жизненного цикла.

- Знать особенности, основные методы и технологии разработки командной стратегии и организации командной работы.

Уметь:

- Уметь осуществлять критический анализ проблемных ситуаций на основе системного подхода.

- Уметь управлять проектом на всех этапах его жизненного цикла.

- Уметь применять знания по выработке командной стратегии организации работы в команде.

Владеть:

- Владеть навыками выработки стратегий действий.

-

- Владеть навыками организации и руководства работой команды.

2. Место дисциплины "Управление проектами" в структуре ОПОП магистратуры

Для освоения дисциплины необходимы компетенции (знания умения, навыки и (или) опыт профессиональной деятельности), сформированные в рамках изучения следующих дисциплин: Основы научных исследований, Менеджмент профессиональной деятельности.

Дисциплина входит в Блок 1 «Дисциплины (модули)» ОПОП. Цель дисциплины - получение обучающимися знаний, умений, навыков и (или) опыта профессиональной деятельности, необходимых для формирования компетенций, указанных в пункте 1.

МИНОБРНАУКИ РОССИИ

федеральное государственное бюджетное образовательное учреждение
высшего образования

«Кузбасский государственный технический университет имени Т. Ф. Горбачева»

Аннотация к рабочей программе дисциплины

Философские проблемы науки и техники

Направление подготовки «10.04.01 Информационная безопасность»
Направленность (профиль) подготовки «01 Организация и технология защиты информации»

Присваиваемая квалификация
"Магистр"

Формы обучения
очная

Кемерово 2025 г.

1. Перечень планируемых результатов обучения по дисциплине "Философские проблемы науки и техники", соотношенных с планируемыми результатами освоения образовательной программы

Освоение дисциплины направлено на формирование:
универсальных компетенций:

УК-5 - Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия

Знать: 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: 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: 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.

В результате освоения дисциплины обучающийся в общем по дисциплине должен

Знать:

- 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:

- 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:

- 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.

2. Место дисциплины "Философские проблемы науки и техники" в структуре ОПОП магистратуры

Для освоения дисциплины необходимы компетенции (знания умения, навыки и (или) опыт профессиональной деятельности), сформированные в рамках изучения следующих дисциплин: Основы научных исследований.

Дисциплина входит в Блок 1 «Дисциплины (модули)» ОПОП. Цель дисциплины - получение обучающимися знаний, умений, навыков и (или) опыта профессиональной деятельности, необходимых для формирования компетенций, указанных в пункте 1.

МИНОБРНАУКИ РОССИИ

федеральное государственное бюджетное образовательное учреждение
высшего образования

«Кузбасский государственный технический университет имени Т. Ф. Горбачева»

Аннотация к рабочей программе дисциплины

Государственная тайна и защита информации

Направление подготовки «10.04.01 Информационная безопасность»
Направленность (профиль) подготовки «01 Организация и технология защиты информации»

Присваиваемая квалификация
"Магистр"

Формы обучения
очная

Кемерово 2025 г.

1. Перечень планируемых результатов обучения по дисциплине "Государственная тайна и защита информации", соотнесенных с планируемыми результатами освоения образовательной программы

Освоение дисциплины направлено на формирование:
профессиональных компетенций:

ПК-3 - Владеет нормативно-методической базой обеспечения защиты сведений, составляющих государственную тайну

Знать: Знать требования правовых актов в области защиты государственной тайны и информационной безопасности, режима секретности

Уметь: Уметь соблюдать в профессиональной деятельности требования правовых актов в области защиты информации и сведений составляющих государственную тайну

Владеть: Владеть навыками обеспечения соблюдения режима секретности

В результате освоения дисциплины обучающийся в общем по дисциплине должен

Знать:

- Знать требования правовых актов в области защиты государственной тайны и информационной безопасности, режима секретности

Уметь:

- Уметь соблюдать в профессиональной деятельности требования правовых актов в области защиты информации и сведений составляющих государственную тайну

Владеть:

- Владеть навыками обеспечения соблюдения режима секретности

2. Место дисциплины "Государственная тайна и защита информации" в структуре ОПОП магистратуры

Для освоения дисциплины необходимы компетенции (знания умения, навыки и (или) опыт профессиональной деятельности), сформированные в рамках изучения следующих дисциплин: Управление информационной безопасностью, Организационно-распорядительная документация по обеспечению информационной безопасности, Управление инцидентами информационной безопасности, Технологии обеспечения информационной безопасности.

Дисциплина входит в Блок 1 «Дисциплины (модули)» ОПОП. Цель дисциплины - получение обучающимися знаний, умений, навыков и (или) опыта профессиональной деятельности, необходимых для формирования компетенций, указанных в пункте 1.

МИНОБРНАУКИ РОССИИ

федеральное государственное бюджетное образовательное учреждение
высшего образования

«Кузбасский государственный технический университет имени Т. Ф. Горбачева»

Аннотация к рабочей программе дисциплины

Защищенные информационные системы

Направление подготовки «10.04.01 Информационная безопасность»
Направленность (профиль) подготовки «01 Организация и технология защиты информации»

Присваиваемая квалификация
"Магистр"

Формы обучения
очная

Кемерово 2025 г.

1. Перечень планируемых результатов обучения по дисциплине "Защищенные информационные системы", соотнесенных с планируемыми результатами освоения образовательной программы

Освоение дисциплины направлено на формирование:
общефессиональных компетенций:

ОПК-1 - Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;

Знать: 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.

Уметь: 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: 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;

Знать: 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.

Уметь: 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: Владеть навыками технических проектов систем (подсистемы либо компонента системы) обеспечения информационной безопасности.

В результате освоения дисциплины обучающийся в общем по дисциплине должен

Знать:

- 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.

- 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.

Уметь:

- 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

- 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:

- Владеть навыками разработки комплексной инфраструктуры защищенной информационной системы, навыками разработки проектов нормативных и правовых актов предприятия, учреждения, организации, регламентирующих деятельность по обеспечению ИБ.

- Владеть навыками технических проектов систем (подсистемы либо компонента системы) обеспечения информационной безопасности.

2. Место дисциплины "Защищенные информационные системы" в структуре ОПОП магистратуры

Для освоения дисциплины необходимы компетенции (знания умения, навыки и (или) опыт профессиональной деятельности), сформированные в рамках изучения следующих дисциплин: .

Дисциплина входит в Блок 1 «Дисциплины (модули)» ОПОП. Цель дисциплины - получение обучающимися знаний, умений, навыков и (или) опыта профессиональной деятельности, необходимых для формирования компетенций, указанных в пункте 1.

МИНОБРНАУКИ РОССИИ

федеральное государственное бюджетное образовательное учреждение
высшего образования

«Кузбасский государственный технический университет имени Т. Ф. Горбачева»

Аннотация к рабочей программе дисциплины

Информационная безопасность интернета вещей

Направление подготовки «10.04.01 Информационная безопасность»
Направленность (профиль) подготовки «01 Организация и технология защиты информации»

Присваиваемая квалификация
"Магистр"

Формы обучения
очная

Кемерово 2025 г.

1. Перечень планируемых результатов обучения по дисциплине "Информационная безопасность интернета вещей", соотнесенных с планируемыми результатами освоения образовательной программы

Освоение дисциплины направлено на формирование:
общефессиональных компетенций:

ОПК-2 - Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности;

Знать: Знает принципы построения систем на базе IoT-устройств, 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 IoT-устройств и протоколов передачи данных; средства обеспечения информационной безопасности IoT-систем; принципы построения защищенных телекоммуникационных систем; механизмы реализации атак в сетях Интернета вещей;

Уметь: 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.

Владеть: 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 IoT-устройств; планировать разработку сложных системы на базе IoT-устройств; проводить выбор эффективных способов реализации структур системы на базе IoT-устройств при решении профессиональных задач.

В результате освоения дисциплины обучающийся в общем по дисциплине должен

Знать:

- Знает принципы построения систем на базе IoT-устройств, 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 IoT-устройств и протоколов передачи данных; средства обеспечения информационной безопасности IoT-систем; принципы построения защищенных телекоммуникационных систем; механизмы реализации атак в сетях Интернета вещей;

Уметь:

- 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.

Владеть:

- 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 IoT-устройств; планировать разработку сложных системы на базе IoT-устройств; проводить выбор эффективных способов реализации структур системы на базе IoT-устройств при решении профессиональных задач.

2. Место дисциплины "Информационная безопасность интернета вещей" в структуре ОПОП магистратуры

Для освоения дисциплины необходимы компетенции (знания умения, навыки и (или) опыт профессиональной деятельности), сформированные в рамках изучения следующих дисциплин: .

Дисциплина входит в Блок 1 «Дисциплины (модули)» ОПОП. Цель дисциплины - получение обучающимися знаний, умений, навыков и (или) опыта профессиональной деятельности, необходимых для формирования компетенций, указанных в пункте 1.

МИНОБРНАУКИ РОССИИ

федеральное государственное бюджетное образовательное учреждение
высшего образования

«Кузбасский государственный технический университет имени Т. Ф. Горбачева»

Аннотация к рабочей программе дисциплины

Искусственный интеллект

Направление подготовки «10.04.01 Информационная безопасность»
Направленность (профиль) подготовки «01 Организация и технология защиты информации»

Присваиваемая квалификация
"Магистр"

Формы обучения
очная

Кемерово 2025 г.

1. Перечень планируемых результатов обучения по дисциплине "Искусственный интеллект", соотнесенных с планируемыми результатами освоения образовательной программы

Освоение дисциплины направлено на формирование:
универсальных компетенций:

УК-2 - Способен управлять проектом на всех этапах его жизненного цикла

Знать: Знает основы построения информационно-вычислительных систем; перечень конструкций и библиотек языков программирования, принципов построения программ в процедурно-ориентированной и объектно-ориентированной парадигмах.

Уметь: Умеет реализовывать алгоритмы на языке программирования, осуществлять работы с интегрированной средой разработки программного обеспечения, проводить оценку вычислительной сложности.

Владеть: Владеет навыками работы с интегрированной средой разработки программного обеспечения, определения вычислительной сложности реализуемых алгоритмов.

В результате освоения дисциплины обучающийся в общем по дисциплине должен

Знать:

- Знает основы построения информационно-вычислительных систем; перечень конструкций и библиотек языков программирования, принципов построения программ в процедурно-ориентированной и объектно-ориентированной парадигмах.

Уметь:

- Умеет реализовывать алгоритмы на языке программирования, осуществлять работы с интегрированной средой разработки программного обеспечения, проводить оценку вычислительной сложности.

Владеть:

- Владеет навыками работы с интегрированной средой разработки программного обеспечения, определения вычислительной сложности реализуемых алгоритмов.

2. Место дисциплины "Искусственный интеллект" в структуре ОПОП магистратуры

Для освоения дисциплины необходимы компетенции (знания умения, навыки и (или) опыт профессиональной деятельности), сформированные в рамках изучения следующих дисциплин: .

Дисциплина входит в Блок 1 «Дисциплины (модули)» ОПОП. Цель дисциплины - получение обучающимися знаний, умений, навыков и (или) опыта профессиональной деятельности, необходимых для формирования компетенций, указанных в пункте 1.

МИНОБРНАУКИ РОССИИ

федеральное государственное бюджетное образовательное учреждение
высшего образования

«Кузбасский государственный технический университет имени Т. Ф. Горбачева»

Аннотация к рабочей программе дисциплины

Менеджмент профессиональной деятельности

Направление подготовки «10.04.01 Информационная безопасность»
Направленность (профиль) подготовки «01 Организация и технология защиты информации»

Присваиваемая квалификация
"Магистр"

Формы обучения
очная

Кемерово 2025 г.

1. Перечень планируемых результатов обучения по дисциплине "Менеджмент профессиональной деятельности", соотношенных с планируемыми результатами освоения образовательной программы

Освоение дисциплины направлено на формирование:
универсальных компетенций:

УК-3 - Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели

Знать: Знать основы работы в команде и порядок выработки командной стратегии для достижения поставленной цели.

Уметь: Уметь организовывать и руководить работой команды.

Владеть: 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

Знать: Знать основы определения приоритетов и способы совершенствования собственной деятельности.

Уметь: Уметь определять и реализовывать приоритеты собственной деятельности.

Владеть: Владеть способностью совершенствовать собственную деятельность на основе самооценки.

В результате освоения дисциплины обучающийся в общем по дисциплине должен

Знать:

- Знать основы работы в команде и порядок выработки командной стратегии для достижения поставленной цели.

- Знать основы определения приоритетов и способы совершенствования собственной деятельности.

Уметь:

- Уметь организовывать и руководить работой команды.

- Уметь определять и реализовывать приоритеты собственной деятельности.

Владеть:

- Владеть навыками руководства работой команды и выработки командной стратегии для достижения поставленной цели.

- Владеть способностью совершенствовать собственную деятельность на основе самооценки.

2. Место дисциплины "Менеджмент профессиональной деятельности" в структуре ОПОП магистратуры

Для освоения дисциплины необходимы компетенции (знания умения, навыки и (или) опыт профессиональной деятельности), сформированные в рамках изучения следующих дисциплин: .

Дисциплина входит в Блок 1 «Дисциплины (модули)» ОПОП. Цель дисциплины - получение обучающимися знаний, умений, навыков и (или) опыта профессиональной деятельности, необходимых для формирования компетенций, указанных в пункте 1.

МИНОБРНАУКИ РОССИИ

федеральное государственное бюджетное образовательное учреждение
высшего образования

«Кузбасский государственный технический университет имени Т. Ф. Горбачева»

Аннотация к рабочей программе дисциплины

Организационно-распорядительная документация по обеспечению информационной безопасности

Направление подготовки «10.04.01 Информационная безопасность»
Направленность (профиль) подготовки «01 Организация и технология защиты информации»

Присваиваемая квалификация
"Магистр"

Формы обучения
очная

Кемерово 2025 г.

1. Перечень планируемых результатов обучения по дисциплине "Организационно-распорядительная документация по обеспечению информационной безопасности", соотнесенных с планируемыми результатами освоения образовательной программы

Освоение дисциплины направлено на формирование:
общефессиональных компетенций:

ОПК-3 - Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности;

Знать: Знать источники правовой информации, виды нормативных правовых актов, стандарты в области информационной безопасности.

Уметь: Уметь анализировать, изучать и обобщать правовую информацию, определять релевантные для профессиональной деятельности нормативные акты, использовать нормативные и методические документы при оформлении технической документации.

Владеть: 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.

В результате освоения дисциплины обучающийся в общем по дисциплине должен

Знать:

- Знать источники правовой информации, виды нормативных правовых актов, стандарты в области информационной безопасности.

Уметь:

- Уметь анализировать, изучать и обобщать правовую информацию, определять релевантные для профессиональной деятельности нормативные акты, использовать нормативные и методические документы при оформлении технической документации.

Владеть:

- 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.

2. Место дисциплины "Организационно-распорядительная документация по обеспечению информационной безопасности" в структуре ОПОП магистратуры

Для освоения дисциплины необходимы компетенции (знания умения, навыки и (или) опыт профессиональной деятельности), сформированные в рамках изучения следующих дисциплин: Управление информационной безопасностью, Управление инцидентами информационной безопасности, Построение моделей угроз информационной безопасности.

Дисциплина входит в Блок 1 «Дисциплины (модули)» ОПОП. Цель дисциплины - получение обучающимися знаний, умений, навыков и (или) опыта профессиональной деятельности, необходимых для формирования компетенций, указанных в пункте 1.

МИНОБРНАУКИ РОССИИ

федеральное государственное бюджетное образовательное учреждение
высшего образования

«Кузбасский государственный технический университет имени Т. Ф. Горбачева»

Аннотация к рабочей программе дисциплины

Организация защиты объектов информатизации

Направление подготовки «10.04.01 Информационная безопасность»
Направленность (профиль) подготовки «01 Организация и технология защиты информации»

Присваиваемая квалификация
"Магистр"

Формы обучения
очная

Кемерово 2025 г.

1. Перечень планируемых результатов обучения по дисциплине "Организация защиты объектов информатизации", соотнесенных с планируемыми результатами освоения образовательной программы

Освоение дисциплины направлено на формирование:
профессиональных компетенций:

ПК-1 - Владеет методикой проведения предпроектного обследования объектов информатизации и выделенных(защищаемых) помещений

Знать: 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.

Уметь: Умеет разрабатывать организационно-распорядительные документы по обеспечению безопасности значимых объектов критической информационной инфраструктуры.

Владеть: Владеет техническими мерами обеспечения безопасности значимых объектов критической информационной инфраструктуры.

ПК-2 - Способен приводить аналитическое обоснование необходимости создания систем защиты информации

Знать: Знает общие принципы организации защиты объектов критической информационной инфраструктуры и ее частей.

Уметь: Умеет организовывать защиту объектов критической информационной инфраструктуры и ее частей с учетом действующих нормативных и методических документов.

Владеть: 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

Знать: Знает нормативную базу, регламентирующую процессы аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации

Уметь: Умеет разрабатывать организационно-распорядительные документы по сопровождению процессов аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации

Владеть: Имеет опыт организации аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации

В результате освоения дисциплины обучающийся в общем по дисциплине должен

Знать:

- Знает нормативную базу, регламентирующую процессы аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации

- 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.

- Знает общие принципы организации защиты объектов критической информационной инфраструктуры и ее частей.

Уметь:

- Умеет разрабатывать организационно-распорядительные документы по сопровождению процессов аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации

-

- Умеет разрабатывать организационно-распорядительные документы по обеспечению безопасности значимых объектов критической информационной инфраструктуры.

- Умеет организовывать защиту объектов критической информационной инфраструктуры и ее частей с учетом действующих нормативных и методических документов.

Владеть:

- Имеет опыт организации аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации

- Владеет техническими мерами обеспечения безопасности значимых объектов критической

информационной инфраструктуры.

- Владеет методикой определения категории объектов критической информационной инфраструктуры.

2. Место дисциплины "Организация защиты объектов информатизации" в структуре ОПОП магистратуры

Для освоения дисциплины необходимы компетенции (знания умения, навыки и (или) опыт профессиональной деятельности), сформированные в рамках изучения следующих дисциплин: Управление информационной безопасностью, Защищенные информационные системы, Организационно-распорядительная документация по обеспечению информационной безопасности, Управление инцидентами информационной безопасности, Построение моделей угроз информационной безопасности, Технологии обеспечения информационной безопасности.

Дисциплина входит в Блок 1 «Дисциплины (модули)» ОПОП. Цель дисциплины - получение обучающимися знаний, умений, навыков и (или) опыта профессиональной деятельности, необходимых для формирования компетенций, указанных в пункте 1.

МИНОБРНАУКИ РОССИИ

федеральное государственное бюджетное образовательное учреждение
высшего образования

«Кузбасский государственный технический университет имени Т. Ф. Горбачева»

Аннотация к рабочей программе дисциплины

Организация приемочных испытаний системы защиты информации

Направление подготовки «10.04.01 Информационная безопасность»
Направленность (профиль) подготовки «01 Организация и технология защиты информации»

Присваиваемая квалификация
"Магистр"

Формы обучения
очная

Кемерово 2025 г.

1. Перечень планируемых результатов обучения по дисциплине "Организация приемочных испытаний системы защиты информации", соотнесенных с планируемыми результатами освоения образовательной программы

Освоение дисциплины направлено на формирование:
профессиональных компетенций:

ПК-5 - Способен организовывать и проводить приемочные испытания СЗИ, вводить в эксплуатацию СЗИ

Знать: Нормативную базу регламентирующую приемочные испытания СЗИ при вводе в эксплуатацию СЗИ

Уметь: Умеет организовывать приемочные испытания системы защиты информации

Владеть: Методами организации приемочных испытаний системы защиты информации

В результате освоения дисциплины обучающийся в общем по дисциплине должен

Знать:

- Нормативную базу регламентирующую приемочные испытания СЗИ при вводе в эксплуатацию СЗИ

Уметь:

- Умеет организовывать приемочные испытания системы защиты информации

Владеть:

- Методами организации приемочных испытаний системы защиты информации

2. Место дисциплины "Организация приемочных испытаний системы защиты информации" в структуре ОПОП магистратуры

Для освоения дисциплины необходимы компетенции (знания умения, навыки и (или) опыт профессиональной деятельности), сформированные в рамках изучения следующих дисциплин: Управление информационной безопасностью, Организационно-распорядительная документация по обеспечению информационной безопасности, Сертификация средств защиты информации, Управление инцидентами информационной безопасности, Построение моделей угроз информационной безопасности, Технологии обеспечения информационной безопасности.

Дисциплина входит в Блок 1 «Дисциплины (модули)» ОПОП. Цель дисциплины - получение обучающимися знаний, умений, навыков и (или) опыта профессиональной деятельности, необходимых для формирования компетенций, указанных в пункте 1.

МИНОБРНАУКИ РОССИИ

федеральное государственное бюджетное образовательное учреждение
высшего образования

«Кузбасский государственный технический университет имени Т. Ф. Горбачева»

Аннотация к рабочей программе дисциплины

Основы научных исследований

Направление подготовки «10.04.01 Информационная безопасность»
Направленность (профиль) подготовки «01 Организация и технология защиты информации»

Присваиваемая квалификация
"Магистр"

Формы обучения
очная

Кемерово 2025 г.

1. Перечень планируемых результатов обучения по дисциплине "Основы научных исследований", соотношенных с планируемыми результатами освоения образовательной программы

Освоение дисциплины направлено на формирование:
общефессиональных компетенций:

ОПК-4 - Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок;

Знать: Знает основные формы, методы и приемы научного исследования области безопасности объектов критической информационной инфраструктуры.

Уметь: 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.

Владеть: 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.

Знать: 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 исследований и обработка их результатов.

Уметь: Уметь применять методы научных исследований ; организовывать научные исследования; проводить экспериментальные исследования и обрабатывать их результаты.

Владеть: Владеть методами научных исследований ; организации научных исследований; навыками экспериментальных исследований и обработки их результатов.

универсальных компетенций:

УК-4 - Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия

Знать: 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

Уметь: Составлять документы и научные тексты по результатам научного исследования в соответствии с требованиями, установленными нормами, особенностями стилей речи и стандартами.

Владеть: Применяет языковые нормы при составлении документов и научных текстов по исследованию безопасности объектов критической информационной инфраструктуры.

В результате освоения дисциплины обучающийся в общем по дисциплине должен

Знать:

- 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 исследований и обработка их результатов.

- 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

- Знает основные формы, методы и приемы научного исследования области безопасности объектов критической информационной инфраструктуры.

Уметь:

- Уметь применять методы научных исследований ; организовывать научные исследования; проводить экспериментальные исследования и обрабатывать их результаты.

- Составлять документы и научные тексты по результатам научного исследования в соответствии с требованиями, установленными нормами, особенностями стилей речи и стандартами.

- 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.

Владеть:

- Владеть методами научных исследований ; организации научных исследований; навыками экспериментальных исследований и обработки их результатов.

- Применяет языковые нормы при составлении документов и научных текстов по исследованию безопасности объектов критической информационной инфраструктуры.

- Демонстрирует способности анализа наборов данных при помощи различных сред их анализа с наглядной визуализацией получаемых результатов

2. Место дисциплины "Основы научных исследований" в структуре ОПОП магистратуры

Для освоения дисциплины необходимы компетенции (знания умения, навыки и (или) опыт профессиональной деятельности), сформированные в рамках изучения следующих дисциплин: .

Дисциплина входит в Блок 1 «Дисциплины (модули)» ОПОП. Цель дисциплины - получение обучающимися знаний, умений, навыков и (или) опыта профессиональной деятельности, необходимых для формирования компетенций, указанных в пункте 1.

МИНОБРНАУКИ РОССИИ

федеральное государственное бюджетное образовательное учреждение
высшего образования

«Кузбасский государственный технический университет имени Т. Ф. Горбачева»

Аннотация к рабочей программе дисциплины

Проектирование систем (компонента системы) обеспечения информационной безопасности

Направление подготовки «10.04.01 Информационная безопасность»

Направленность (профиль) подготовки «01 Организация и технология защиты информации»

Присваиваемая квалификация

"Магистр"

Формы обучения

очная

Кемерово 2025 г.

1. Перечень планируемых результатов обучения по дисциплине "Проектирование систем (компонента системы) обеспечения информационной безопасности", соотнесенных с планируемыми результатами освоения образовательной программы

Освоение дисциплины направлено на формирование:
общефессиональных компетенций:

ОПК-2 - Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности;

Знать: 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: 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: 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.

В результате освоения дисциплины обучающийся в общем по дисциплине должен

Знать:

- 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:

- 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:

- 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.

2. Место дисциплины "Проектирование систем (компонента системы) обеспечения информационной безопасности" в структуре ОПОП магистратуры

Для освоения дисциплины необходимы компетенции (знания умения, навыки и (или) опыт профессиональной деятельности), сформированные в рамках изучения следующих дисциплин: Управление информационной безопасностью, Защищенные информационные системы, Организационно-распорядительная документация по обеспечению информационной безопасности, Управление инцидентами информационной безопасности, Построение моделей угроз информационной безопасности, Технологии обеспечения информационной безопасности.

Дисциплина входит в Блок 1 «Дисциплины (модули)» ОПОП. Цель дисциплины - получение обучающимися знаний, умений, навыков и (или) опыта профессиональной деятельности, необходимых для формирования компетенций, указанных в пункте 1.

МИНОБРНАУКИ РОССИИ

федеральное государственное бюджетное образовательное учреждение
высшего образования

«Кузбасский государственный технический университет имени Т. Ф. Горбачева»

Аннотация к рабочей программе дисциплины

Сертификация средств защиты информации

Направление подготовки «10.04.01 Информационная безопасность»
Направленность (профиль) подготовки «01 Организация и технология защиты информации»

Присваиваемая квалификация
"Магистр"

Формы обучения
очная

Кемерово 2025 г.

1. Перечень планируемых результатов обучения по дисциплине "Сертификация средств защиты информации", соотнесенных с планируемыми результатами освоения образовательной программы

Освоение дисциплины направлено на формирование:
профессиональных компетенций:

ПК-3 - Владеет нормативно-методической базой обеспечения защиты сведений, составляющих государственную тайну

Знать: 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: 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: Владеть схемами сертификации и правилами декларирования соответствия; признаками обязательной и добровольной сертификации.

В результате освоения дисциплины обучающийся в общем по дисциплине должен

Знать:

- 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:

- 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:

- Владеть схемами сертификации и правилами декларирования соответствия; признаками обязательной и добровольной сертификации.

2. Место дисциплины "Сертификация средств защиты информации" в структуре ОПОП магистратуры

Для освоения дисциплины необходимы компетенции (знания умения, навыки и (или) опыт профессиональной деятельности), сформированные в рамках изучения следующих дисциплин: Управление информационной безопасностью, Защищенные информационные системы, Управление инцидентами информационной безопасности, Построение моделей угроз информационной безопасности.

Дисциплина входит в Блок 1 «Дисциплины (модули)» ОПОП. Цель дисциплины - получение обучающимися знаний, умений, навыков и (или) опыта профессиональной деятельности, необходимых для формирования компетенций, указанных в пункте 1.

МИНОБРНАУКИ РОССИИ

федеральное государственное бюджетное образовательное учреждение
высшего образования

«Кузбасский государственный технический университет имени Т. Ф. Горбачева»

Аннотация к рабочей программе дисциплины

Технологии обеспечения информационной безопасности

Направление подготовки «10.04.01 Информационная безопасность»
Направленность (профиль) подготовки «01 Организация и технология защиты информации»

Присваиваемая квалификация
"Магистр"

Формы обучения
очная

Кемерово 2025 г.

1. Перечень планируемых результатов обучения по дисциплине "Технологии обеспечения информационной безопасности", соотнесенных с планируемыми результатами освоения образовательной программы

Освоение дисциплины направлено на формирование:
общефессиональных компетенций:

ОПК-1 - Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;

Знать: 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.

Уметь: 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.

Владеть: 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;

Знать: Знает принципы эксплуатации средств защиты информации. Знает методы тестирования средств защиты информационной безопасности

Уметь: 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.

Владеть: Имеет опыт разработки требования к средствам и методам контроля проектируемой системы (подсистемы либо компонента системы) обеспечения информационной безопасности

В результате освоения дисциплины обучающийся в общем по дисциплине должен

Знать:

- 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.

- Знает принципы эксплуатации средств защиты информации. Знает методы тестирования средств защиты информационной безопасности

Уметь:

- 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.

-

- 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.

Владеть:

- Владеет опытом настройки средства защиты информации в соответствии с требованиями к объекту защиты с целью снижения рисков информационной безопасности.

-

- Имеет опыт разработки требования к средствам и методам контроля проектируемой системы (подсистемы либо компонента системы) обеспечения информационной безопасности

2. Место дисциплины "Технологии обеспечения информационной безопасности" в структуре ОПОП магистратуры

Для освоения дисциплины необходимы компетенции (знания умения, навыки и (или) опыт профессиональной деятельности), сформированные в рамках изучения следующих дисциплин: Управление информационной безопасностью, Защищенные информационные системы, Построение моделей угроз информационной безопасности.

Дисциплина входит в Блок 1 «Дисциплины (модули)» ОПОП. Цель дисциплины - получение обучающимися знаний, умений, навыков и (или) опыта профессиональной деятельности, необходимых для формирования компетенций, указанных в пункте 1.

МИНОБРНАУКИ РОССИИ

федеральное государственное бюджетное образовательное учреждение
высшего образования

«Кузбасский государственный технический университет имени Т. Ф. Горбачева»

Аннотация к рабочей программе дисциплины

Управление информационной безопасностью

Направление подготовки «10.04.01 Информационная безопасность»
Направленность (профиль) подготовки «01 Организация и технология защиты информации»

Присваиваемая квалификация
"Магистр"

Формы обучения
очная

Кемерово 2025 г.

1. Перечень планируемых результатов обучения по дисциплине "Управление информационной безопасностью", соотнесенных с планируемыми результатами освоения образовательной программы

Освоение дисциплины направлено на формирование:
общефессиональных компетенций:

ОПК-1 - Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;

Знать: Знать основные принципы организации технического, программного и информационного 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: 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: 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 оценки 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;

Знать: 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

Уметь: 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

Владеть: Владеет навыками разработки политики информационной безопасности различных уровней

В результате освоения дисциплины обучающийся в целом по дисциплине должен

Знать:

- 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

- Знать основные принципы организации технического, программного и информационного 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:

- 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

- 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:

- Владеет навыками разработки политики информационной безопасности различных уровней

- 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 оценки информационных рисков; методами организации и управления деятельностью служб защиты информации на предприятии; навыками управления информационной безопасностью простых объектов.

2. Место дисциплины "Управление информационной безопасностью" в структуре ОПОП магистратуры

Для освоения дисциплины необходимы компетенции (знания умения, навыки и (или) опыт профессиональной деятельности), сформированные в рамках изучения следующих дисциплин: .

В области Дисциплина входит в Блок 1 «Дисциплины (модули)» ОПОП. Цель дисциплины - получение обучающимися знаний, умений, навыков и (или) опыта профессиональной деятельности, необходимых для формирования компетенций, указанных в пункте 1.

МИНОБРНАУКИ РОССИИ

федеральное государственное бюджетное образовательное учреждение
высшего образования

«Кузбасский государственный технический университет имени Т. Ф. Горбачева»

Аннотация к рабочей программе дисциплины

Построение моделей угроз информационной безопасности

Направление подготовки «10.04.01 Информационная безопасность»
Направленность (профиль) подготовки «01 Организация и технология защиты информации»

Присваиваемая квалификация
"Магистр"

Формы обучения
очная

Кемерово 2025 г.

1. Перечень планируемых результатов обучения по дисциплине "Построение моделей угроз информационной безопасности", соотнесенных с планируемыми результатами освоения образовательной программы

Освоение дисциплины направлено на формирование:
профессиональных компетенций:

ПК-6 - Прогнозирует риски в информационной безопасности и управляет инцидентами информационной безопасности

Знать: 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

Уметь: Умеет выявлять и оценивать актуальности угроз информационной безопасности, построения их моделей для определения требований о защите информации

Владеть: Владеет навыками работы с нормативными документами по определению требований о защите информации компьютерных систем.

В результате освоения дисциплины обучающийся в общем по дисциплине должен

Знать:

- 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

Уметь:

- Умеет выявлять и оценивать актуальности угроз информационной безопасности, построения их моделей для определения требований о защите информации

Владеть:

- Владеет навыками работы с нормативными документами по определению требований о защите информации компьютерных систем.

2. Место дисциплины "Построение моделей угроз информационной безопасности" в структуре ОПОП магистратуры

Для освоения дисциплины необходимы компетенции (знания умения, навыки и (или) опыт профессиональной деятельности), сформированные в рамках изучения следующих дисциплин: .

Дисциплина входит в Блок 1 «Дисциплины (модули)» ОПОП. Цель дисциплины - получение обучающимися знаний, умений, навыков и (или) опыта профессиональной деятельности, необходимых для формирования компетенций, указанных в пункте 1.

МИНОБРНАУКИ РОССИИ

федеральное государственное бюджетное образовательное учреждение
высшего образования

«Кузбасский государственный технический университет имени Т. Ф. Горбачева»

Аннотация к программе практики

Вид практики: Производственная

Тип практики: Преддипломная практика

Способ проведения: стационарная и(или) выездная

Направление подготовки «10.04.01 Информационная безопасность»

Направленность (профиль) подготовки «01 Организация и технология защиты информации»

Присваиваемая квалификация

"Магистр"

Формы обучения

очная

Кемерово 2026

Определения, сокращения и аббревиатуры

В данной программе практики приняты следующие сокращения:

ВКР - выпускная квалификационная работа;

ЗЕ - зачетная единица;

НЕУД - неудовлетворительно;

ОПОП - основная профессиональная образовательная программа;

ОТЛ - отлично;

ОФ - очная форма обучения;

ОЗФ - очно-заочная форма обучения;

ПК - профессиональная компетенция;

УД - удовлетворительно;

ХОР - хорошо.

1 Формы и способы проведения практики

Способ проведения практики: стационарная и(или) выездная.

Форма проведения практики: непрерывно - путем выделения в календарном учебном графике непрерывного периода учебного времени для проведения всех видов практик, предусмотренных ОПОП ВО.

Тип практики: Преддипломная практика.

2 Перечень планируемых результатов обучения при прохождении практики, соотнесенных с планируемыми результатами освоения ОПОП

Прохождение практики направлено на формирование компетенций:

ПК-1 - Владеет методикой проведения предпроектного обследования объектов информатизации и выделенных(защищаемых) помещений

Знать:

Уметь: Уметь выполнять проектирование и разработку систем, комплексов, средств и технологий обеспечения информационной безопасности.

Владеть: Владеть навыками работы в среде CASE-средств анализа и проектирования систем навыками использования в практической деятельности новых знаний и умений.

Иметь опыт: Иметь опыт проведения предпроектного обследования объектов информатизации и выделенных защищаемых помещений.

ПК-2 - Способен приводить аналитическое обоснование необходимости создания систем защиты информации

Знать:

Уметь: Уметь проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты.

Владеть: Владеть навыками обеспечения информационной безопасностью объектов защиты.

Иметь опыт: Иметь опыт приведения аналитическое обоснование необходимости создания систем защиты информации.

ПК-3 - Владеет нормативно-методической базой обеспечения защиты сведений, составляющих государственную тайну

Знать:

Уметь: 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: Владеть знаниями законодательных и правовых актов в области безопасности; правилами составления локальных нормативных актов и регламентов в области информационной безопасности.

Иметь опыт: 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

Знать:

Уметь: Уметь проводить экспериментальные исследования защищенности объектов, разрабатывать требования к защите от утечек по техническим каналам.

Владеть: Владеть методами инструментального контроля защищенности объекта.

Иметь опыт: 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

Знать:

Уметь: Уметь организовывать приемочные испытания системы защиты информации.

Владеть: Владеть способами приемочных испытаний СЗИ, ввода в эксплуатацию СЗИ.

Иметь опыт: Иметь опыт организации приемочных испытаний систем защиты информации.

ПК-6 - Прогнозирует риски в информационной безопасности и управляет инцидентами информационной безопасности

Знать:

Уметь: Уметь организовать процесс управления информационной безопасностью.

Владеть: Владеть навыками управления системой информационной безопасности.

Иметь опыт: Иметь опыт анализа рисков в информационной безопасности и управлении инцидентами информационной безопасности.

УК-1 - Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, выработать стратегию действий

Знать:

Уметь: Уметь анализировать необходимую информацию в области информационной безопасности, содержащуюся в различных формах отчетности и прочих отечественных и зарубежных источника.

Владеть: Владеть навыками интерпретации информации, содержащейся в различных отечественных и зарубежных источниках в области информационной безопасности.

Иметь опыт: Иметь опыт анализа проблемных ситуаций на основе системного подхода

МИНОБРНАУКИ РОССИИ

федеральное государственное бюджетное образовательное учреждение
высшего образования

«Кузбасский государственный технический университет имени Т. Ф. Горбачева»

Аннотация к программе практики

Вид практики: Производственная

Тип практики: Организационно-управленческая практика

Способ проведения: стационарная и(или) выездная

Направление подготовки «10.04.01 Информационная безопасность»

Направленность (профиль) подготовки «01 Организация и технология защиты информации»

Присваиваемая квалификация

"Магистр"

Формы обучения

очная

Кемерово 2026

Определения, сокращения и аббревиатуры

В данной программе практики приняты следующие сокращения:

ВКР - выпускная квалификационная работа;

ЗЕ - зачетная единица;

НЕУД - неудовлетворительно;

ОПОП - основная профессиональная образовательная программа;

ОТЛ - отлично;

ОФ - очная форма обучения;

ОЗФ - очно-заочная форма обучения;

ПК - профессиональная компетенция;

УД - удовлетворительно;

ХОР - хорошо.

1 Формы и способы проведения практики

Способ проведения практики: стационарная и(или) выездная.

Форма проведения практики: непрерывно - путем выделения в календарном учебном графике непрерывного периода учебного времени для проведения всех видов практик, предусмотренных ОПОП ВО.

Тип практики: Организационно-управленческая практика.

2 Перечень планируемых результатов обучения при прохождении практики, соотнесенных с планируемыми результатами освоения ОПОП

Прохождение практики направлено на формирование компетенций:

ПК-3 - Владеет нормативно-методической базой обеспечения защиты сведений, составляющих государственную тайну

Знать:

Уметь: Уметь использовать полученные знания в профессиональной деятельности.

Владеть: Владеть нормативно-методической базой обеспечения защиты сведений, составляющих государственную тайну.

Иметь опыт: 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

Знать:

Уметь: Уметь подготавливать объекты вычислительной техники и выделенные (защищаемые) помещения к аттестации по требованиям безопасности информации.

Владеть: Владеть методами подготовки объектов вычислительной техники и выделенных (защищаемых) помещений к аттестации.

Иметь опыт: 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

Знать:

Уметь: Уметь организовывать приемочные испытания системы защиты информации

Владеть: Владеть способами приемочных испытаний СЗИ, ввода в эксплуатацию СЗИ.

Иметь опыт: Иметь опыт организации приемочных испытаний систем защиты информации.

ПК-6 - Прогнозирует риски в информационной безопасности и управляет инцидентами информационной безопасности

Знать:

Уметь: 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: Владеть методами разработки мер безопасности, контрмер и действий по каждой актуальной угрозе для снижения уровня риска, управлять инцидентами информационной безопасности.

Иметь опыт: Иметь опыт определения риска в информационной безопасности и управления инцидентами

информационной безопасности.

УК-2 - Способен управлять проектом на всех этапах его жизненного цикла

Знать:

Уметь: Уметь моделировать риски.

Владеть: Владеть пониманием структуры и системы взаимосвязи процессов управления.

Иметь опыт: 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

Знать:

Уметь: Уметь организовывать работу команды по подготовке проекта организационно-распорядительной документации на системы защиты информации.

Владеть: Владеть методами организации мер, обеспечивающих эффективность системы защиты информации.

Иметь опыт: Иметь опыт организации обучения персонала использованию технических, программных (программно-технических) средств защиты информации.

МИНОБРНАУКИ РОССИИ

федеральное государственное бюджетное образовательное учреждение
высшего образования

«Кузбасский государственный технический университет имени Т. Ф. Горбачева»

Аннотация к программе практики

Вид практики: Производственная

Тип практики: Проектно-технологическая практика

Способ проведения: стационарная и(или) выездная

Направление подготовки «10.04.01 Информационная безопасность»

Направленность (профиль) подготовки «01 Организация и технология защиты информации»

Присваиваемая квалификация

"Магистр"

Формы обучения

очная

Кемерово 2026

Определения, сокращения и аббревиатуры

В данной программе практики приняты следующие сокращения:

ВКР - выпускная квалификационная работа;

ЗЕ - зачетная единица;

НЕУД - неудовлетворительно;

ОПОП - основная профессиональная образовательная программа;

ОТЛ - отлично;

ОФ - очная форма обучения;

ОЗФ - очно-заочная форма обучения;

ПК - профессиональная компетенция;

УД - удовлетворительно;

ХОР - хорошо.

1 Формы и способы проведения практики

Способ проведения практики: стационарная и(или) выездная.

Форма проведения практики: дискретно - путем чередования в календарном учебном графике периодов учебного времени для проведения практик с периодами учебного времени для проведения теоретических занятий.

Тип практики: Проектно-технологическая практика.

2 Перечень планируемых результатов обучения при прохождении практики,соотнесенных с планируемыми результатами освоения ОПОП

Прохождение практики направлено на формирование компетенций:

ОПК-1 - Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;

Знать:

Уметь: Уметь определять информационные ресурсы, подлежащие защите информации, угрозы безопасности информации.

Владеть: Владеть профессиональной терминологией в области обеспечения безопасности персональных данных; методами мониторинга и аудита, выявления угроз и управления информационной безопасностью.

Иметь опыт: 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;

Знать:

Уметь: Уметь отечественные и зарубежные стандарты в области компьютерной безопасности и информационной безопасности объектов для проектирования, разработки и оценки защищенности компьютерных систем.

Владеть: Владеть методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.

Иметь опыт: 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;

Знать:

Уметь: 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: Владеть навыками оформления рабочей технической документации.

Иметь опыт: 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;

Знать:

Уметь: Уметь проектировать и сопровождать типовые специализированные автоматизированные информационные системы, локальные сети; осуществлять подготовку технико-экономических обоснований соответствующих проектных решений.

Владеть: Владеть навыками определения затрат компании на информационную безопасность и проведения зависимости между затратами и уровнем защищенности.

Иметь опыт: 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.

Знать:

Уметь: 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: Владеть навыками выполнения расчетов, обработки результатов экспериментов, оценки погрешностей и достоверности результатов, навыками проведения экспериментально-исследовательских работ системы защиты информации.

Иметь опыт: Иметь опыт оформления научно-технических отчетов, обзоров, результатов выполненных исследований, научных докладов и статей.

