МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

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

Институт информационных технологий, машиностроения и автотранспорта

УТВЕРЖДАЮ

И.о. директора ИТМА

_____ Жданов В.Л.

«31» августа 2026г.

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ИГОТОВОЙ (ГОСУДАРСТВЕННОЙ ИТОГОВОЙ) АТТЕСТАЦИИ

Направление подготовки 10.04.01 Информационная безопасность

Направленность (профиль) «Организация и технология защиты информации»

Присваиваемая квалификация: «Магистр»

Блок 3 «Государственная итоговая аттестация»

«Подготовка к процедуре защиты и защита выпускной квалификационной работы»

Формы обучения Очная, очно-заочная

Кемерово 2026

Оценочные материалы для проведения итоговой (государственной итоговой) аттестации составили

Заведующий кафедрой	Информационной безопасности		Прокопенко Е.В.
должность	кафедра	подпись	ФИО

Оценочные материалы для проведения итоговой (государственной итоговой) аттестации обсуждены на заседании кафедры информационной безопасности и согласованы учебно-методической комиссией направления подготовки 10.04.01 Информационная безопасность Протокол № 1 от «31» августа 2026г.

Заведующий кафедрой, Председатель учебно-методической комиссии направления подготовки 10.04.01 Информационная безопасность	Информационной безопасности		Прокопенко Е.В.
должность	кафедра	подпись	ФИО

Оглавление

1. Оценочные материалы для проведения итоговой (государственной итоговой) аттестации

Настоящий оценочные материалы для проведения итоговой (государственной итоговой) аттестации (ОМ для ГИА) является приложением к программе государственной итоговой аттестации. ОМ для ГИА позволяет определить соответствие результатов освоения обучающимся основной профессиональной образовательной программы соответствующим требованиям федерального государственного образовательного стандарта.

2. Перечень оценочных средств

Для определения качества освоения обучающимися основной профессиональной образовательной программы используются следующие оценочные средства:

Оценочное средство	**Краткая характеристика оценочного средства**	**Представление оценочного средства в ФОС**
Выпускная квалификационная работа	Выпускная квалификационная работа представляет собой работу, демонстрирующую уровень подготовленности выпускника к самостоятельной профессиональной деятельности	Критерии оценки результатов защиты выпускной квалификационной работы

3. Перечень компетенций, которыми должны овладеть обучающиеся в результате

В результате освоения образовательной программы у обучающихся должны быть сформированы следующие компетенции:

Код компетенции	**Наименование компетенции**
Универсальные компетенции	
УК-1	Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий
УК-2	Способен управлять проектом на всех этапах его жизненного цикла
УК-3	Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели
УК-4	Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия
УК-5	Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия
УК-6	Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки
Общепрофессиональные компетенции	
ОПК-1	Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;
ОПК-2	Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности;
ОПК-3	Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности;

Код компетенции	Наименование компетенции
ОПК-4	Способен осуществлять сбор, обработку и анализ 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.
Профессиональные компетенции	
Тип задач профессиональной деятельности: проектный	
ПК-1	Владеет методикой проведения предпроектного обследования объектов информатизации и выделенных(защищаемых) помещений
ПК-2	Способен приводить аналитическое обоснование необходимости создания систем защиты информации
Тип задач профессиональной деятельности: организационно-управленческий	
ПК-3	Владеет нормативно-методической базой 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
ПК-5	Способен организовывать и проводить приемочные испытания СЗИ, вводить в эксплуатацию СЗИ
ПК-6	Прогнозирует риски в информационной безопасности и управляет инцидентами информационной безопасности

4. Описание индикаторов достижения компетенций (показателей и критериев оценивания компетенций), используемых для оценивания результатов обучения при освоении образовательной программы

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

Код и содержание компетенции	Индикаторы достижения компетенции	Результаты обучения
ПК-1 Владеть методикой проведения предпроектного обследования объектов информатизации и выделенных(защищаемых) помещений	Владеть методикой проведения предпроектного обследования объектов информатизации и выделенных(защищаемых) помещений	Знать содержание и порядок деятельности персонала объектов критической информационной инфраструктуры и ее частей. Знать нормативную базу, регламентирующую процессы обеспечения информационной безопасности объектов критической информационной инфраструктуры и ее частей. Уметь разрабатывать организационно-распорядительные документы по обеспечению безопасности значимых объектов критической информационной инфраструктуры. Владеть 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	Знать общие принципы организации защиты объектов критической информационной инфраструктуры и ее частей. Уметь организовывать защиту объектов критической информационной инфраструктуры и ее частей с учетом действующих нормативных и методических документов. Владеть 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	Знать нормативную базу, регламентирующую процессы аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации Уметь 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
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. Уметь организовывать приемочные испытания системы защиты информации. Владеть методами организация приемочных испытаний системы защиты информации.

Код и содержание компетенции	Индикаторы достижения компетенции	Результаты обучения
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	Знать общую информацию об угрозах и нарушителях безопасности информации компьютерных систем. Знать методику выявления и оценки актуальности угроз информационной безопасности, построения их моделей для определения требований о защите информации. Уметь выявлять и оценивать актуальности угроз информационной безопасности, построения их моделей для определения требований о защите информации. Владеть навыками работы с нормативными документами по определению требований о защите информации компьютерных систем.
Управление инцидентами информационной безопасности		
ПК-6 Прогнозирует риски в информационной безопасности и управляет инцидентами информационной безопасности	Прогнозирует риски в информационной безопасности и управляет инцидентами информационной безопасности.	Знать нормативные акты и стандарты в области управления инцидентами информационной безопасности. Уметь выполнять планирование, идентификацию и анализ инцидентов информационной безопасности, моделировать риски, проводить мониторинг, осуществлять адекватное реагирование на различные инциденты. Владеть специализированным программным обеспечением, пониманием структуры и системы взаимосвязи процессов управления инцидентами информационной безопасности.
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,	Знать особенности управления проектом на всех стадиях и этапах жизненного цикла. Уметь управлять проектом на всех этапах его жизненного цикла.

Код и содержание компетенции	Индикаторы достижения компетенции	Результаты обучения
	обосновывает актуальность, значимость, ожидаемые результаты и возможные сферы их применения.	
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.	Знать принципы разработки защищенных информационных систем различного применения и степени сложности. Знать методики выявления угроз и оценки уязвимостей информационных систем. Знать методы и средства обеспечения информационной безопасности, а также нормативную базу регламентирующую классификацию данных средств. Знать типовые требования к разработке средств защиты, направленные на снижение рисков информационной безопасности. Уметь обосновывать требования к процессам и технологиям обеспечения информационной безопасности объектов критической

Код и содержание компетенции	Индикаторы достижения компетенции	Результаты обучения
		информационной инфраструктуры. Уметь осуществлять выбор подсистем, реализующих технологии обеспечения информационной безопасности для объектов критической информационной инфраструктуры. Уметь обосновывать требования к мерам обеспечения информационной безопасности объектов критической информационной инфраструктуры. Уметь составлять техническое задание по разработке систем, комплексов, средств и технологий обеспечения информационной безопасности. Уметь 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.	Знать принципы организации и этапы разработки системы (подсистемы либо компонента системы) обеспечения информационной безопасности объектов критической информационной инфраструктуры. Знать методики испытаний средств и систем обеспечения информационной безопасности. Уметь составлять требования и критерии оценки информационной безопасности. Уметь разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности объектов критической информационной инфраструктуры. Уметь разрабатывать требования к средствам и методам контроля проектируемой системы (подсистемы либо компонента системы) обеспечения информационной безопасности объектов критической информационной инфраструктуры. Уметь 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	Обосновывает требования к системе обеспечения информационной безопасности и разрабатывает проекты технического задания на ее	Знать основные принципы организации технического, программного и информационною обеспечения защищенных информационных систем; основные механизмы информационной безопасности и типовые процессы управления этими

Код и содержание компетенции	Индикаторы достижения компетенции	Результаты обучения
на ее создание	создание.	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	Знать нормативную и правовую базу в области управления информационной безопасностью объектов критической информационной инфраструктуры. Знать отечественные и зарубежные стандарты в области управления информационной безопасностью объектов критической информационной инфраструктуры. Знать структуру политик обеспечения

Код и содержание компетенции	Индикаторы достижения компетенции	Результаты обучения
		информационной безопасности объектов критической информационной инфраструктуры и требования к их содержанию Уметь разрабатывать проекты нормативных и организационно-распорядительных документов по обеспечению информационной безопасности объектов критической информационной инфраструктуры. Уметь разрабатывать политику информационной безопасности объектов критической информационной инфраструктуры различных уровней Владеть 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	Знать основные формы, методы и приемы научного исследования области безопасности объектов критической информационной инфраструктуры. Уметь составлять план научного исследования в области безопасности объектов критической информационной инфраструктуры и проводить деятельность в соответствии с составленным планом. Уметь 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	Знать принципы построения устного и письменного высказывания на русском и иностранном(ых) языках, правила и закономерности деловой устной и письменной коммуникации; Владеть широким словарным запасом, достаточным для осуществления деловой коммуникации в рамках академической и профессиональной направленности Составлять документы и научные тексты по результатам научного

Код и содержание компетенции	Индикаторы достижения компетенции	Результаты обучения
		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	Разрабатывает требования к средствам и методам контроля проектируемой системы (подсистемы либо	Знать принципы построения систем на базе IoT-устройств, а также способы их эффективной реализации; существующие технологии в области Интернета вещей;

Код и содержание компетенции	Индикаторы достижения компетенции	Результаты обучения
компонента системы) обеспечения информационной безопасности;	компонента системы) обеспечения информационной безопасности.	стандарты реализации интерфейсов подключаемых устройств; стандарты информационного взаимодействия систем. Знать 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 проводить анализ защищенности IoT-систем; Разрабатывать модели угроз для систем Интернета Вещей. Уметь 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 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 .	Знать технологии обеспечения информационной безопасности. Знать основные виды уязвимостей систем и угрозы информационной безопасности. Знать методы и средства обеспечения информационной безопасности, а также нормативную базу регламентирующую классификацию данных средств. Уметь обосновывать выбор средств защиты информации для противодействия конкретным угрозам. Уметь осуществлять подбор средств защиты информации в соответствии с заданными критериями. Уметь обосновывать требования к мерам обеспечения

Код и содержание компетенции	Индикаторы достижения компетенции	Результаты обучения
		информационной безопасности в соответствии с нормативной базой. Уметь составлять техническое задание по обеспечению информационной безопасности на объекте с использованием сертифицированных ФСТЭК средств защиты информации. Владеть 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	Знать принципы эксплуатации средств защиты информации. Знать методы тестирования средств защиты информационной безопасности . Уметь осуществлять настройку режимов работы средств защиты информации в соответствии с определенными моделями угроз. Уметь разрабатывать сценарии тестирования средств защиты информации. Уметь разрабатывать требования к средствам защиты информации. Владеть 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 Владеть 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

Код и содержание компетенции	Индикаторы достижения компетенции	Результаты обучения
		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 управляет инцидентами информационной безопасности.
УК-2 Способен управлять проектом на всех этапах его жизненного цикла	Управляет 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 Владеть 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

Код и содержание компетенции	Индикаторы достижения компетенции	Результаты обучения
		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 Владеть 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

Код и содержание компетенции	Индикаторы достижения компетенции	Результаты обучения
		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 управляет 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	Способен разработать проекты организационно-	Знать требования основных действующих государственных стандартов (ГОСТ)

Код и содержание компетенции	Индикаторы достижения компетенции	Результаты обучения
организационно-распорядительных документов по обеспечению информационной безопасности;	распорядительных документов по обеспечению информационной безопасности.	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 Владеть нормативно-методической базой обеспечения защиты сведений, составляющих	Владеет нормативно-методической базой обеспечения защиты сведений, составляющих	Знать нормативно-правовое обеспечение сертификации технических и программных средств защиты информации, правила лицензирования и сертификации в области

Код и содержание компетенции	Индикаторы достижения компетенции	Результаты обучения
государственную тайну	государственную тайну.	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.	Знать основы построения информационно-вычислительных систем; перечень конструкций и библиотек языков программирования, принципов построения программ в процедурно-ориентированной и объектно-ориентированной парадигмах. Уметь реализовывать алгоритмы на языке программирования, осуществлять работы с интегрированной средой разработки программного обеспечения, проводить оценку вычислительной сложности. Владеть навыками работы с интегрированной средой разработки программного обеспечения, определения вычислительной сложности реализуемых алгоритмов.

5. Содержание оценочных средств государственной итоговой аттестации

Государственная итоговая аттестация проводится в форме защиты выпускной квалификационной работы (ВКР).

Выпускная квалификационная работа (Далее – ВКР) представляет собой выполненную обучающимся (несколькими обучающимися совместно) работу, демонстрирующую уровень подготовленности выпускника к самостоятельной профессиональной деятельности.

5.1. Критерии оценки результатов защиты выпускной квалификационной работы

Во время защиты обучающемуся задаются вопросы, касающиеся темы ВКР, а также другие вопросы, позволяющие оценить сформированность заявленных в образовательной программе компетенций.

Критерии оценивания результатов подготовки и защиты выпускной квалификационной работы (ВКР):

- обучающийся сделал уверенный доклад по ВКР, дал правильные и полные ответы более чем на 85 % заданных вопросов – 85…100 баллов;
- обучающийся сделал не уверенный доклад по ВКР, но дал правильные и полные ответы не менее чем на 85 % заданных вопросов или обучающийся сделал уверенный доклад по ВКР, но дал правильные и полные ответы более чем на 75 %, но не более чем на 85 % заданных вопросов – 75…84 балла;

− обучающийся сделал не уверенный доклад по ВКР, но дал правильные и полные ответы более чем на 75 %, но не более чем на 85 % заданных вопросов или обучающийся сделал уверенный доклад по ВКР, но дал правильные и полные ответы более чем на 60 %, но не более чем на 75 % заданных вопросов – 60…74 балла;

− в прочих случаях – 0…59 баллов.

Шкала оценивания:

Количество баллов	0…59	60…74	75…84	85…100
Шкала оценивания	Неудовлетворительно	Удовлетворительно	Хорошо	Отлично

5.2. Типовые вопросы, позволяющие раскрыть полноту выполнения разделов ВКР:

1. Поясните, по каким показателям производился общий структурный анализ и классификация объекта информатизации / объекта защиты?
2. Какие методики использовались для анализа защищенности объекта информатизации / объекта защиты?
3. Какие методики использовались для анализа угроз объекта информатизации / объекта защиты?
4. Какие методики использовались для анализа уязвимостей объекта информатизации / объекта защиты?
5. Какие методики использовались для построения модели угроз?
6. Каковы границы периметра защиты объекта информатизации / объекта защиты?
7. Сформулируйте требования к СЗИ для защиты объекта информатизации / объекта защиты?
8. Какая модель доступа используется в объекте информатизации / объекте защиты?
9. Какая модель политики межсетевого экрана используется для защиты от вторжений из внешней сети?
10. Как реализован комплекс организационно-административных мероприятий для защиты объекта информатизации / объекта защиты?

5.3. Типовые вопросы, позволяющие оценить сформированность заявленных в образовательной программе компетенций.

Код компетенции	Наименование компетенции	Вопросы для оценки компетенций
Универсальные компетенции		
УК-1	Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	1. Что планируется делать, если при сканировании сети АИС обнаружена уязвимость? 2. Что планируется делать, если обнаружена сетевая атака?
УК-2	Способен управлять проектом на всех этапах его жизненного цикла	1. Как осуществляется выбор модели при разработке АСЗИ или СЗИ? 2. Какие бывают методики описания бизнес-процессов, потоков данных, работ в АИС?

Код компетенции	Наименование компетенции	Вопросы для оценки компетенций
УК-3	Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	1. Какие методы существуют для описания целей, стратегий? 2. Как эффективно распределить обязанности в команде?
УК-4	Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	1. Какие программные / браузерные переводчики можно использовать для перевода печатного текста в области ИБ? 2. Какие переводчики для мобильных устройств можно использовать для перевода голосовой информации в области ИБ?
УК-5	Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	1. Каковы основы теории коммуникации, проблемы культурной идентичности и межкультурных контактов? 2. Как достигать эффективности коммуникации, использовать общие коды (вербальные или невербальные)?
УК-6	Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки	1. Каковы движущие силы развития личности? 2. Каковы значимые черты личности?
Общепрофессиональные компетенции		
ОПК-1	Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;	1. Чем информационная безопасность отличается от кибербезопасности? 2. Какие уязвимости информационных систем или ПО вы знаете?
ОПК-2	Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности;	1. В каких нормативных документах можно найти шаблоны отчетные документы и разделы технических заданий на создание систем защиты информации автоматизированных систем? 2. Какие сведения указываются в отчетных документах и разделах технических заданий на создание систем защиты информации автоматизированных систем?
ОПК-3	Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности;	1. В каких нормативных документах можно найти шаблоны отчетные документы и разделы технических заданий на создание систем защиты информации автоматизированных систем?

Код компетенции	Наименование компетенции	Вопросы для оценки компетенций
		2. Какие сведения указываются в отчетных документах и разделах технических заданий на создание систем защиты информации автоматизированных систем?
ОПК-4	Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок;	1. Какие критерии при анализе характера обрабатываемой информации являются наиболее важными? 2. Как формируется перечень информации, подлежащей защите?
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.	1. Как с помощью дедуктивного анализа провести расследование инцидента по кейсу? 2. Как для заданного кейса определить необходимость и конкретные средства криптографии?
Профессиональные компетенции		
Тип задач профессиональной деятельности: проектный		
ПК-1	Владеет методикой проведения предпроектного обследования объектов информатизации и выделенных(защищаемых) помещений	1. На какой стадии жизненного цикла объекта информатизации проводится его аттестация по требованиям безопасности информации? 2. Допускается ли проведение аттестации объекта информатизации после ввода его в эксплуатацию?
ПК-2	Способен приводить аналитическое обоснование необходимости создания систем защиты информации	1. В каких случаях необходимо использовать криптографические средства защиты информации? 2. Что является критерием обоснованности использования криптографических средств защиты информации?
Тип задач профессиональной деятельности: организационно-управленческий		
ПК-3	Владеет нормативно-методической базой обеспечения защиты сведений, составляющих государственную тайну	1. Перечислите основные документы по защите информации в РФ 2. Перечислите основные документы по защите персональных данных (ПДн) в РФ
ПК-4	Способен организовывать и сопровождать аттестацию объектов вычислительной техники и выделенных	1. Какие существуют группы методов для защиты информации ограниченного доступа в АС? 2. Назовите нормативные

Код компетенции	Наименование компетенции	Вопросы для оценки компетенций
	(защищаемых) помещений на соответствие требованиям по защите информации	документы, регламентирующие защиту информации ограниченного доступа в АС
ПК-5	Способен организовывать и проводить приемочные испытания СЗИ, вводить в эксплуатацию СЗИ	3. Как осуществляется выбор модели при разработке АСЗИ или СЗИ? 4. Какие бывают методики описания бизнес-процессов, потоков данных, работ в АИС?
ПК-6	Прогнозирует риски в информационной безопасности и управляет инцидентами информационной безопасности	1. Что представляет собой определение, оценка, анализ и управление рисками информационной безопасности? 2. Опишите подходы к анализу и структурных и функциональных схем защищенных автоматизированных информационных систем.

5.4. Основные качественные показатели оценивания ВКР:

- актуальность и обоснование выбора темы ВКР;
- логика работы, соответствия содержания ВКР и её темы;
- степень самостоятельности;
- достоверность и обоснованность выводов;
- качество оформления ВКР, четкость и грамотность изложения материала;
- качество доклада, наглядных материалов (презентации), умение вести полемику по теоретическим и практическим вопросам, глубина и правильность ответов на вопросы членов ГЭК и замечания рецензентов;
- список использованных источников, достаточность использования отечественной и зарубежной литературы;
- возможность внедрения.

Показатель оценивания	Критерий			
	Отлично	Хорошо	Удовлетворительно	Неудовлетворительно
Актуальность и обоснование выбора темы	Работа выполнена на актуальную тему и решает практическую задачу, соответствующую профилю направления подготовки	Работа выполнена на актуальную тему и решает практическую задачу	В работе не определены решаемые практические задачи	Тема работы неактуальна и не соответствует профилю направления подготовки
Логика работы, соответствие содержания и темы	Все разделы работы соответствуют теме, логически выстроена последовательность решения проблемы, решены все поставленные задачи	Все разделы работы соответствуют теме, определены задачи решения исследуемой проблематики, решены основные поставленные задачи	Разделы работы соответствуют теме работы, поставленные задачи не позволяют решить исследуемую проблему	Последовательность разделов работы выстроена нелогично, содержание не соответствует теме работы

Показатель оценивания	Критерий			
	Отлично	**Хорошо**	**Удовлетворительно**	**Неудовлетворительно**
Степень самостоятельности	Все поставленные руководителем ВКР задачи решены самостоятельно в полном объеме	Поставленные руководителем ВКР задачи решены самостоятельно с частичным его участием	Поставленные руководителем ВКР задачи решены самостоятельно со значительным его участием	Не решены поставленные руководителем задачи
Достоверность и обоснованность выводов	Выводы достоверны и обоснованы, подтверждены необходимыми расчетами, решены все поставленные задачи	Выводы достоверны и обоснованы, подтверждены необходимыми расчетами	Не все выводы подтверждены необходимыми расчетами	Выводы не обоснованы, не подтверждены расчетами
Качество оформления ВКР	Оформление ВКР полностью соответствует установленным требованиям	Оформление ВКР имеет незначительные отклонения от установленных требований	Оформление ВКР имеет значительные отклонения от установленных требований	Оформление ВКР не соответствует установленным требованиям
Качество доклада, наглядных материалов (презентации)	Качество доклада высокое, в докладе представлены все результаты, доклад выполнен с использованием компьютерных технологий в виде презентации	Качество доклада хорошее, в докладе представлены все результаты, доклад выполнен с использованием компьютерных технологий в виде презентации	Качество доклада удовлетворительное, в докладе представлены не все результаты, доклад выполнен с использованием компьютерных технологий в виде презентации	Качество доклада неудовлетворительное, в докладе не представлены результаты, доклад выполнен с использованием компьютерных технологий в виде презентации низкого качества
Список использованных источников	Использованные источники актуальны и соответствуют тематике работы, все источники использованы в работе	Использованные источники актуальны и соответствуют тематике работы, не все источники использованы в работе	Не все использованные источники актуальны и соответствуют тематике работы, не все источники использованы в работе	Использованные источники не актуальны и не все соответствуют тематике работы, не все источники использованы в работе
Возможность внедрения	Результаты ВКР представляют практическую значимость и ценность, могут быть использованы на предприятии и(или) в образовательном процессе	Результаты ВКР могут быть использованы на предприятии и(или) в образовательном процессе	Результаты ВКР соответствуют требованиям, предъявляемым к работам бакалавров и достаточны для защиты ВКР	Результаты ВКР не представляют значимость и ценность, не имеют возможность внедрения

5.5. Примерный перечень тем выпускных квалификационных работ:

1. Проект формирования комплекса средств для проведения аттестационных испытаний АСЗИ / СЗИ для решения задач…..
2. Проект формирования комплекса средств для проведения анализа защищенности АСЗИ / СЗИ….
3. Проект формирования комплекса средств для проведения пентестинга АСЗИ /СЗИ….
4. Исследование методов гарантированного уничтожения данных на различных аппаратных и программных платформах

5. Анализ инцидентов информационной безопасности с применением методов Threat Intelligence
6. Система поиска открытых прокси-серверов в сети интернет
7. Анализ методов защиты приложений от отладки на основе технологии VMProtect.
8. Анализ стойкости защиты приложений от нелицензионного использования на основе электронных ключей SenseLock
9. Разработка системы моделирования и исследования DoS-атак
10. Исследование кибератак на АСУ ТП на примере модели угледобывающего предприятия
11. Методика анализа аппаратно-программных комплексов интернета вещей для сбора информации о структурно-функциональных характеристиках данных систем
12. Исследование методов и средств восстановления удаленных данных в целях обнаружения доказательств совершения преступлений
13. Исследование методов составления профайла на физическое лицо или организацию на основе технологии разведки по открытым источникам (OSINT)
14. Исследование уязвимостей биометрических систем аутентификации пользователей
15. Исследование вопросов безопасности мультипотоковой передачи данных на примере протокола MPTCP
16. Исследование безопасности предприятий информационных услуг
17. Исследование возможностей создания защищенной инфраструктуры малого предприятия
18. Исследование методов анонимизации конфиденциальной информации
19. Анализ возможностей СЗИ для аудита ИТ-инфраструктуры предприятия
20. Исследование возможностей СЗИ (Технологии) для создания надежных каналов удаленного доступа в различных операционных средах
21. Анализ развития и возможности использования сетей с нулевым доверием
22. Анализ возможностей кибератак на нейросети в системах машинного зрения
23. Исследование возможностей шлюза безопасности UserGate (либо другого вендора / решения) для обеспечения защиты информации, циркулирующей в корпоративной сети предприятия
24. Исследование возможности создания защищенного канала связи применительно к облачным технологиям
25. Анализ и выбор коммутационного оборудования для системы ИБ Организации
26. Оценка рисков ИБ корпоративной сети Организации
27. Анализ защищенности web-приложения на основе моделирования сетевых атак
28. Сравнительный анализ DLP-систем
29. Исследование возможностей СЗИ как платформы для SIEM системы в корпоративной сети
30. Сравнительный анализ средств защиты Web-приложений и выработка рекомендаций по их использованию на предприятии
31. Анализ и предотвращение кибератак на компьютерные сети
32. Анализ и прогнозирование угроз безопасности информации
33. Анализ и обеспечение безопасности при использовании блокчейн-технологий в банковском секторе

34. Анализ угроз безопасности персональных данных, циркулирующих в подсистеме АСУ «*Предприятие*»

35. Разработка системы контроля и мониторинга почтового трафика «Предприятие»

36. Анализ способов предотвращения внутренних утечек информации

37. Разработка информационной модели подготовки муниципальной бюджетной организации к проверкам регуляторов в области защиты информации на примере «Предприятие»

38. Организация работ по защите персональных данных в «Предприятие»