МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Сибирский государственный университет геосистем и технологий»

Кафедра информационной безопасности

ПРОГРАММА ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

Направление подготовки
10.04.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Профиль подготовки
Организация и управление информационной безопасностью

УРОВЕНЬ ВЫСШЕГО ОБРАЗОВАНИЯ
МАГИСТРАТУРА

Новосибирск - 2023

Программа государственной итоговой аттестации по направлению подготовки 10.04.01 Информационная безопасность (уровень магистратуры) составлена на основании федерального государственного образовательного стандарта высшего образования, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 26 ноября 2020 г. №1455 и учебного плана профиля «Организация и управление информационной безопасностью».

Составители:

Новиков Сергей Николаевич, профессор кафедры информационной безопасности, д.т.н., доцент; Троеглазова Анна Владимировна, доцент кафедры информационной безопасности, PhD

Программа государственной итоговой аттестации обсуждена и одобрена на заседании кафедры *информационной безопасности*

Зав. кафедрой ИБ _____ Троеглазова А.В.
(подпись)

Программа одобрена ученым советом *Института оптики и технологий информационной безопасности*

Председатель Ученого совета ИОиТИБ _____ А.В. Шабурова
(подпись)

«СОГЛАСОВАНО»

Зав. библиотекой СГУГиТ _____ А.В. Шпак
(подпись)

ОГЛАВЛЕНИЕ

1 ОБЩИЕ ПОЛОЖЕНИЯ

Государственная итоговая аттестация (далее – ГИА) представляет собой форму оценки степени и уровня освоения обучающимися основной образовательной программы, которая проводится на основе принципов объективности и независимости оценки качества подготовки обучающихся.

В соответствии с Федеральным законом Российской Федерации «Об образовании в Российской Федерации» от 29.12.2012 г. № 273-ФЗ итоговая аттестация, завершающая освоение основных образовательных программ, является обязательной и проводится в порядке и в форме, которые установлены образовательной организацией. Порядок и форма ГИА установлены локальными нормативными актами СГУГиТ.

К ГИА допускаются обучающийся, не имеющий академической задолженности и в полном объеме выполнивший учебный план или индивидуальный учебный план.

Успешное прохождение ГИА является основанием для выдачи обучающемуся документа о высшем образовании и о квалификации образца, установленного Министерством науки и высшего образования Российской Федерации.

Обучающиеся, не прошедшие государственное аттестационное испытание в связи с неявкой на государственное аттестационное испытание по неуважительной причине или в связи с получением оценки "неудовлетворительно", отчисляются из организации с выдачей справки об обучении как не выполнившие обязанностей по добросовестному освоению образовательной программы и выполнению учебного плана.

К проведению ГИА по основным образовательным программам привлекаются представители работодателей или их объединений.

2 ЦЕЛИ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

ГИА проводится в целях определения соответствия результатов освоения обучающимися ООП соответствующим требованиям федерального государственного образовательного стандарта по направлению подготовки 10.04.01 Информационная безопасность (уровень магистратуры), профиль «Организация и управление информационной безопасностью»

Задачами ГИА являются:

– оценка степени и уровня освоения обучающимися ООП по направлению подготовки 10.04.01 Информационная безопасность;

– принятие решения о присвоении квалификации (степени) по результатам ГИА и выдаче документа об образовании и о квалификации;

– проверка готовности выпускника к профессиональной деятельности;

– разработка предложений, направленных на дальнейшее улучшение качества подготовки выпускников, совершенствование организации, содержания, методики и материально-технического обеспечения образовательного процесса.

ГИА проводится на завершающем этапе обучения после прохождения теоретического обучения и всех видов практик, предусмотренных учебным планом по направлению подготовки 10.04.01 Информационная безопасность, профиль «Организация и управление информационной безопасностью».

ГИА по направлению подготовки 10.04.01 Информационная безопасность, профиль «Организация и управление информационной безопасностью» проводится в форме защиты выпускной квалификационной работы (далее – ВКР).

Трудоемкость ГИА составляет 6 зачетных единиц (216 академических часов) и проводится, согласно учебному плану по очно-заочной форме – на 3 курсе.

3 ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

3.1 Перечень компетенций, которыми должны овладеть обучающиеся в результате освоения образовательной программы и индикаторы их достижения

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

Таблица 1

Перечень компетенций

Код компетенции	Содержание формируемой компетенции	Код и наименование индикатора достижения	Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенции	
			Уровни сформированности компетенций	Образовательные результаты
УК-1	Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.1. Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними. УК-1.2. Осуществляет поиск вариантов решения поставленной проблемной ситуации на основе доступных источников информации. УК-1.3. Разрабатывает стратегию достижения поставленной цели как последовательность шагов, предвидя результат каждого из них и оценивая их влияние на внешнее окружение планируемой деятельности и на взаимоотношения участников этой деятельности.	*ПОРОГОВЫЙ («удовлетворительно»)*	*Выпускник знает:* – основные определения, характеристики, составляющие и свойства системы; – основные проблемы в области защиты информации, методы и приемы формализации задач; – постановку основных задач в области проектирования и обеспечения защиты информационных систем, методы и приемы формализации задач; – место и роль общих вопросов систем искусственного интеллекта в научных исследованиях; – современные проблемы математики, физики и экономики; – теоретические модели рассуждений, поведения, обучения; – принципы и методы организации работы в информационно-аналитическом подразделении; – содержание современных философских концепций, их объяснительных ресурсов и методологических возможностей. *Выпускник умеет:* – анализировать задачи, выделяя их базовые составляющие, осуществлять декомпозицию профессиональных задач; – анализировать поставленные задачи по проектированию и обеспечению защищенности информационных систем; – эффективно использовать на практике теоретические компоненты систем искусственного интеллекта; – представлять обзор универсальных методов и законов современного естествознания; – анализировать систему управления информационной безопасностью, выявлять проблемы, осуществлять поиск, критический анализ и синтез информации. *Выпускник владеет:*

				– навыками анализа задач с выделением ее базовых составляющих; – навыками анализа функциональных возможностей защищенных информационных систем; – навыками постановки задач и обработки результатов компьютерного моделирования; – навыками описания процесса управления информационной безопасностью; – навыками поиска и критического анализа информации, необходимой для решения поставленных задач.
			БАЗОВЫЙ («хорошо»)	*Выпускник знает:* – основные определения, характеристики, составляющие и свойства системы; – основные проблемы в области защиты информации, методы и приемы формализации задач; – способы решения задач в области информационной безопасности на основе методологии системного анализа; – постановку основных задач в области проектирования и обеспечения защиты информационных систем, методы и приемы формализации задач; – место и роль общих вопросов систем искусственного интеллекта в научных исследованиях; – современные проблемы математики, физики и экономики; – теоретические модели рассуждений, поведения, обучения; – постановку проблем математического и информационного моделирования сложных систем; – подходы к постановке основных задач по обеспечению защиты информации, методы и приемы формализации задач по управлению информационной безопасностью; – основные источники информации в организации и реализации процесса управления информационной безопасностью; – принципы и методы организации работы в информационно-аналитическом подразделении; – содержание современных философских концепций, их объяснительных ресурсов и методологических возможностей; – специфику, методы и приемы анализа и обобщения социально значимых философских проблем. *Выпускник умеет:* – анализировать задачи, выделяя их базовые

				составляющие, осуществлять декомпозиций профессиональных задач; – осуществлять поиск информации, необходимой для решения задач в области профессиональной деятельности; – использовать системный подход в профессиональной деятельности. – анализировать поставленные задачи по проектированию и обеспечению защищенности информационных систем – эффективно использовать на практике теоретические компоненты систем искусственного интеллекта; – представлять обзор универсальных методов и законов современного естествознания; – применять средства защиты информации; – абстрагироваться от несущественных факторов при моделировании реальных ситуаций в сфере применения информационно-аналитических систем. – анализировать задачи, выделяя их базовые составляющие, осуществлять декомпозиций профессиональных задач в системе управления информационной безопасностью - осуществлять поиск, критический анализ и синтез информации; - выявлять философскую суть конкретных научно-познавательных, социально-политических проблем. – *Выпускник владеет:* – навыками анализа задач с выделением ее базовых составляющих; – навыками применения системного подхода к информационной безопасности; – навыками работы с информацией. навыками анализа функциональных возможностей защищенных информационных систем; – - навыками применения научного подхода при изучении процессов обработки, хранения и передачи информации при эксплуатации защищенных информационных систем – навыками постановки задач и обработки результатов компьютерного моделирования; – – навыками самостоятельной работы в лаборатории на современной вычислительной технике. – навыками анализа задач с выделением ее базовых составляющих; – навыками выбора оптимального способа для решения поставленной задачи. – навыками описания процесса управления информационной безопасности

				– - навыками поиска и критического анализа информации, необходимой для решения поставленной задачи.
			ПОВЫШЕННЫЙ («отлично»)	*Выпускник знает:* – основные определения, характеристики, составляющие и свойства системы; – постановку основных проблем защиты в области защиты информации, методы и приемы формализации задач; – основные источники информации для решения профессиональных задач; – способы решения задач в области информационной безопасности на основе методологии системного анализа. – постановку основных задач в области проектирования и обеспечения защиты информационных систем, методы и приемы формализации задач – место и роль общих вопросов систем искусственного интеллекта в научных исследованиях; – современные проблемы математики, физики и экономики; – теоретические модели рассуждений, поведения, обучения; – постановку проблем математического и информационного моделирования сложных систем; – взаимосвязь естественных и математических наук. – подходы к постановке основных задач по обеспечению защиты информации, методы и приемы формализации задач по управлению информационной безопасностью; – основные источники информации в организации и реализации процесса управления информационной безопасностью; – принципы и методы организации работы в информационно-аналитическом подразделении; – руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации - содержание современных философских концепций, их объяснительных ресурсов и методологических возможностей; - специфику, методы и приемы анализа и обобщения социально значимых философских проблем. – *Выпускник умеет:* – анализировать задачи, выделяя их базовые составляющие, осуществлять декомпозиций

				профессиональных задач; – осуществлять поиск информации, необходимой для решения задач в области профессиональной деятельности; – использовать системный подход в профессиональной деятельности. – анализировать поставленные задачи по проектированию и обеспечению защищенности информационных систем – эффективно использовать на практике теоретические компоненты систем искусственного интеллекта; – представлять обзор универсальных методов и законов современного естествознания; – применять средства защиты информации; – абстрагироваться от несущественных факторов при моделировании реальных ситуаций в сфере применения информационно-аналитических систем; – планировать процесс моделирования и вычислительного эксперимента. – анализировать задачи, выделяя их базовые составляющие, осуществлять декомпозиций профессиональных задач в системе управления информационной безопасностью. – анализировать систему управления информационной безопасностью, выявлять проблемы - осуществлять поиск, критический анализ и синтез информации; - выявлять философскую суть конкретных научно-познавательных, социально-политических проблем; использовать объяснительные ресурсы изученных философских концепций для многостороннего (системного) анализа ситуаций. – *Выпускник владеет:* – навыками анализа задач с выделением ее базовых составляющих; – навыками применения системного подхода к информационной безопасности; – навыками работы с информацией; – навыками выбора оптимального способа для решения поставленной задачи на основе системного подхода. - навыками анализа функциональных возможностей защищенных информационных систем; - навыками применения научного подхода при изучении процессов обработки, хранения и передачи информации при эксплуатации защищенных информационных систем; – - навыками анализа эффективности приме-

				няемых мер защиты информации. – навыками постановки задач и обработки результатов компьютерного моделирования; – – навыками самостоятельной работы в лаборатории на современной вычислительной технике. – навыками анализа задач с выделением ее базовых составляющих; – навыками работы с информацией; – навыками выбора оптимального способа для решения поставленной задачи. – навыками описания процесса управления информационной безопасности – - навыками поиска и критического анализа информации, необходимой для решения поставленной задачи; – навыками критического анализа проблемных ситуаций, выявления их составляющих на основе системного подхода.
УК-2	Способен управлять проектом на всех этапах его жизненного цикла	УК-2.1. Формулирует в рамках обозначенной проблемы, цель, задачи, актуальность, значимость (научную, практическую, методическую и иную в зависимости от типа проекта), ожидаемые результаты и возможные сферы их применения. УК-2.2. Способен представлять результат деятельности и планировать последовательность шагов для достижения данного результата. Формирует план-график реализации проекта в целом и план	*ПОРОГОВЫЙ («удовлетворительно»)*	*Выпускник знает:* – содержание нормативной правовой документации. современные интеллектуальные системы, применяемые для решения задач в области обеспечения информационной безопасности; – - архитектуры нейронных сетей *Выпускник умеет:* – проводить анализ поставленной цели. – обосновывать выбор современных интеллектуальных систем для решения задач в области обеспечения информационной безопасности; – - использовать интеллектуальные методы поиска оптимально эффективных решений *Выпускник владеет:* – методиками разработки целей проекта. – навыками практического применения эволюционного и нейросетевого подходов
			БАЗОВЫЙ («хорошо»)	*Выпускник знает:* – содержание нормативной правовой документации; – методы решения профессиональных задач. – современные интеллектуальные системы, применяемые для решения задач в области обеспечения информационной безопасности; – как планировать последовательность шагов с использованием интеллектуальных технологий в сфере информационной безопасности; - архитектуры нейронных сетей; - принципы применения нейронных сетей в задачах с использованием искусственного интеллекта – *Выпускник умеет:*

		контроля его выполнения. УК-2.3. Организует и координирует работу участников проекта, способствует конструктивному преодолению возникающих разногласий и конфликтов, обеспечивает работу команды необходимыми ресурсами. УК-2.4. Представляет публично результаты проекта (или отдельных его этапов) в форме отчетов, статей, выступлений на научно-практических конференциях, семинарах и т.п.		– проводить анализ поставленной цели, формулировать задачи, необходимые для ее достижения. – обосновывать выбор современных интеллектуальных систем для решения задач в области обеспечения информационной безопасности; - использовать интеллектуальные методы поиска оптимально эффективных решений. – *Выпускник владеет:* – методиками разработки целей и формулировки задач проекта. – навыками практического применения эволюционного и нейросетевого подходов; – - навыками планирования экспериментов при решении традиционных задач с использованием эволюционного и нейросетевого подходов.
			ПОВЫШЕННЫЙ («отлично»)	*Выпускник знает:* – содержание нормативной правовой документации; – методы и способы решения профессиональных задач. – интеллектуальные системы, применяемые для решения задач в области обеспечения информационной безопасности; – как планировать последовательность шагов с использованием интеллектуальных технологий в сфере информационной безопасности; - архитектуры нейронных сетей; - принципы применения нейронных сетей в задачах с использованием искусственного интеллекта; - теоретические основы обучения анализа данных и машинного обучения – *Выпускник умеет:* – проводить анализ поставленной цели, формулировать задачи, необходимые для ее достижения, анализировать альтернативные варианты, используя нормативно-правовую документацию. – обосновывать выбор современных интеллектуальных систем для решения задач в области обеспечения информационной безопасности; – представлять публично результаты проекта; - использовать интеллектуальные методы поиска оптимально эффективных решений; - применять новые методы решения задач с использованием методов искусственного интеллекта в своей проблемной области. – *Выпускник владеет:*

				– методиками разработки целей и формулировки задач проекта, методами оценки потребности в ресурсах, продолжительности и стоимости проекта, навыками работы с нормативно-правовыми документами. – навыками практического применения эволюционного и нейросетевого подходов; – опытом организации и управлением участников проекта; - навыками планирования экспериментов при решении традиционных задач с использованием эволюционного и нейросетевого подходов; – - навыками адекватной оценки сложных ситуаций, оценки рисков и последствий своих действий.
УК-3	Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	УК-3.1. Организует и координирует работу участников проекта, способствует конструктивному преодолению возникающих разногласий и конфликтов. УК-3.2. Учитывает в своей социальной и профессиональной деятельности интересы, особенности поведения и мнения (включая критические) людей, с которыми работает/взаимодействует, в том числе посредством корректировки своих действий. УК-3.3. Предвидит результаты (последствия) как личных, так и коллективных действий.	*ПОРОГОВЫЙ («удовлетворительно»)*	*Выпускник знает:* – основы организации работы специалистов по защите информации в сфере управления информационной безопасностью; - основы организации работы специалистов по моделированию и управлению жизненным циклом информационных систем. - основные понятия в области командной работы – порядок организации работы отдела и специалистов в системе управления информационной безопасностью; основы координации работы специалистов, осуществляющих деятельность в систему управления информационной безопасностью *Выпускник умеет:* – вырабатывать стратегию для достижения цели. - вырабатывать стратегию для реализации процесса управления жизненным циклом информационных систем. - делегировать и распределять трудовые обязанности в команде - вырабатывать стратегию для достижения цели и решения поставленных при организации и реализации деятельности отдела и специалистов в сфере информационной безопасности *Выпускник владеет:* – опытом взаимодействия в профессиональной среде с коллегами и партнерами различного уровня. – опытом взаимодействия в профессиональной среде по вопросам управления жизненным циклом информационных систем. – навыками взаимодействия в конфликтных ситуациях с целью повышения эффективности профессиональной деятельности; – навыками организации своей профессио-

		УК-3.4. Планирует командную работу, распределяет поручения и делегирует полномочия членам команды. Организует обсуждение разных идей и мнений		нальной деятельности – навыками планирования, реализации, проверки и совершенствования системы управления информационной безопасности.
			БАЗОВЫЙ («хорошо»)	*Выпускник знает:* – основы организации и координации работы специалистов в области информационной безопасности; – основы организации и координации работы специалистов по моделированию и управлению жизненным циклом информационных систем. – основные понятия в области информационной безопасности, принципы социальной коммуникации, в том числе в конфликтных ситуациях – порядок организации работы отдела и специалистов в системе управления информационной безопасностью; – основы организации, координации работы специалистов, осуществляющих деятельность в систему управления информационной безопасностью. – *Выпускник умеет:* – вырабатывать стратегию для достижения цели и решения поставленных профессиональных задач; – вырабатывать стратегию для реализации процесса моделирования и управления жизненным циклом информационных систем. – делегировать и распределять трудовые обязанности в команде; – разрабатывать план достижения целей для решения профессиональных задач; – принимать решения в спорных ситуациях. – вырабатывать стратегию для достижения цели и решения поставленных при организации и реализации деятельности отдела и специалистов в сфере информационной безопасности *Выпускник владеет:* – опытом взаимодействия в профессиональной среде с участниками проекта различного уровня; - опытом организации работы по выполнению индивидуальных заданий для решения профессиональных задачи; – опытом взаимодействия в профессиональной среде по вопросам моделирования и управления жизненным циклом информационных систем; - опытом организации работы по выполнению

				индивидуальных заданий при реализации процесса моделирования и управления жизненным циклом информационных систем. – навыками взаимодействия в конфликтных ситуациях с целью повышения эффективности профессиональной деятельности; навыками организации своей профессиональной деятельности – навыками планирования, реализации, проверки и совершенствования системы управления информационной безопасности. навыками принятия управленческих решений и оценки их эффективности.
			ПОВЫШЕННЫЙ («отлично»)	*Выпускник знает:* – основы организации, координации и корректировке работы специалистов по защите информации в сфере управления информационной безопасностью; – основы организации и координации работы специалистов по моделированию и управлению жизненным циклом информационных систем. – основные понятия в области информационной безопасности, принципы социальной коммуникации – порядок организации работы отдела и специалистов в системе управления информационной безопасностью; – основы организации, координации и корректировке работы специалистов, осуществляющих деятельность в систему управления информационной безопасностью. *Выпускник умеет:* – вырабатывать стратегию для достижения цели и решения поставленных задач, распределять временные и кадровые ресурсы для достижения цели; – вырабатывать стратегию для реализации процесса моделирования и управления жизненным циклом информационных систем. – делегировать и распределять трудовые обязанности в команде; – разрабатывать план достижения целей для решения профессиональных задач – вырабатывать стратегию для достижения цели и решения поставленных при организации и реализации деятельности отдела и специалистов в сфере информационной безопасности *Выпускник владеет:* – опытом взаимодействия в профессиональной среде с коллегами и партнерами различного уровня;

				- опытом организации работы по выполнению индивидуальных заданий для решения задач в сфере профессиональной деятельности; - опытом анализа выполненной работы и принятия корректирующих мер по устранению выявленных несоответствий; – опытом взаимодействия в профессиональной среде по вопросам моделирования и управления жизненным циклом информационных систем; - опытом организации работы по выполнению индивидуальных заданий при реализации процесса моделирования и управления жизненным циклом информационных систем; - опытом анализа выполненной работы и принятия корректирующих мер по устранению выявленных несоответствий при реализации процесса моделирования и управления жизненным циклом информационных систем. – навыками взаимодействия в конфликтных ситуациях с целью повышения эффективности профессиональной деятельности; навыками организации своей профессиональной деятельности – навыками планирования, реализации, проверки и совершенствования системы управления информационной безопасности. – навыками принятия управленческих решений и оценки их эффективности. опытом анализа выполненной работы и принятия корректирующих мер по устранению выявленных несоответствий.
УК-4	Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и	УК-4.1. Демонстрирует интегративные умения, необходимые для написания, письменного перевода и редактирования различных академических текстов (рефератов, эссе, обзоров, статей и т.д.) УК-4.2. Представляет результаты академической и профессиональной дея-	*ПОРОГОВЫЙ («удовлетворительно»)*	*Выпускник знает:* - базовую лексику общего языка, лексику нейтрального научного стиля и основную терминологию своей широкой и узкой специальности; некоторые нормы научного иностранного стиля; базовые грамматические правила иностранного языка; правила словообразования в иностранном языке, для удовлетворительного написания, письменного перевода и редактирования несложных академических текстов (рефератов, эссе, обзоров, статей); - базовые коммуникативные технологии, в том числе на иностранном (ых) языке (ах), для осуществления на удовлетворительном уровне академического и профессионального взаимодействия и участия в академических и профессиональных дискуссиях, различных научных мероприятиях, включая международные. *Выпускник умеет:* - применять базовые коммуникативные технологии, в том числе на иностранном (ых) языке

	профессионального взаимодействия	тельности на различных научных мероприятиях, включая международные УК-4.3. Демонстрирует интегративные умения, необходимые для эффективного участия в академических и профессиональных дискуссиях		(ах), для осуществления на удовлетворительном уровне академического и профессионального взаимодействия; - использовать базовую лексику общего языка, лексику нейтрального научного стиля и основную терминологию своей широкой и узкой специальности; некоторые нормы научного иностранного стиля; базовые грамматические правила иностранного языка; правила словообразования в иностранном языке, необходимые для удовлетворительного написания, письменного перевода и редактирования несложных академических текстов (рефератов, эссе, обзоров, статей и т.д.). *Выпускник владеет:* - удовлетворительными навыками написания, письменного перевода и редактирования несложных академических текстов (рефератов, эссе, обзоров, статей и т.д.) - базовыми навыками устной и письменной коммуникации, в том числе на иностранном (ых) языке (ах), для удовлетворительного академического и профессионального взаимодействия и участия в академических и профессиональных дискуссиях, различных научных мероприятиях, включая международные.
			БАЗОВЫЙ («хорошо»)	*Выпускник знает:* - основную лексику общего языка, лексику нейтрального научного стиля и основную терминологию своей широкой и узкой специальности; нормы научного иностранного стиля; грамматические правила иностранного языка; правила словообразования в иностранном языке, необходимые для корректного и обстоятельного написания, письменного перевода и редактирования различных академических текстов (рефератов, эссе, обзоров, статей); - современные коммуникативные технологии, в том числе на иностранном (ых) языке (ах), для содержательного академического и профессионального взаимодействия, для осуществления на должном уровне участия в академических и профессиональных дискуссиях, различных научных мероприятиях, включая международные. *Выпускник умеет:* - применять современные коммуникативные технологии, в том числе на иностранном (ых) языке (ах), для академического и профессионального взаимодействия на хорошем уровне; - представлять результаты академической и профессиональной деятельности на различных научных мероприятиях, включая международные;

				- применять интегративные умения, необходимые для содержательного участия в академических и профессиональных дискуссиях; - использовать без особого затруднения и на хорошем уровне лексику общего языка, лексику нейтрального научного стиля и основную терминологию своей широкой и узкой специальности; нормы научного иностранного стиля; грамматические правила иностранного языка; правила словообразования в иностранном языке, необходимые для корректного написания, письменного перевода и редактирования различных академических текстов (рефератов, эссе, обзоров, статей и т.д.). *Выпускник владеет:* - хорошими навыками написания, письменного перевода и редактирования различных академических текстов (рефератов, эссе, обзоров, статей и т.д.) - навыками устной и письменной коммуникации, в том числе на иностранном (ых) языке (ах), для содержательного академического и профессионального взаимодействия, для осуществления на должном уровне участия в академических и профессиональных дискуссиях, различных научных мероприятиях, включая международные.
			ПОВЫШЕННЫЙ («отлично»)	*Выпускник знает:* - основную лексику общего языка, лексику нейтрального научного стиля и необходимую терминологию своей широкой и узкой специальности; нормы научного иностранного стиля; грамматические правила иностранного языка; правила словообразования в иностранном языке, необходимые для грамотного и эффективного написания, письменного перевода и редактирования различных академических текстов (рефератов, эссе, обзоров, статей); - современные коммуникативные технологии, в том числе на иностранном (ых) языке (ах), для осуществления на высоком уровне академического и профессионального взаимодействия, для эффективного участия в академических и профессиональных дискуссиях, различных научных мероприятиях, включая международные. *Выпускник умеет:* - применять все необходимые современные коммуникативные технологии, в том числе на иностранном (ых) языке (ах), для эффективного академического и профессионального взаимодействия; - представлять на высоком уровне результаты академической и профессиональной деятель-

				ности на различных научных мероприятиях, включая международные; - без затруднений применять интегративные умения, необходимые для эффективного участия в академических и профессиональных дискуссиях; - грамотно и в широком объеме использовать лексику общего языка, лексику нейтрального научного стиля и терминологию своей широкой и узкой специальности; нормы научного иностранного стиля; грамматические правила иностранного языка; правила словообразования в иностранном языке, необходимые для корректного и обстоятельного написания, письменного перевода и редактирования различных академических текстов (рефератов, эссе, обзоров, статей и т.д.). *Выпускник владеет:* - отличными навыками написания, письменного перевода и редактирования различных академических текстов (рефератов, эссе, обзоров, статей и т.д.) - навыками эффективной устной и письменной коммуникации, в том числе на иностранном (ых) языке (ах), для академического и профессионального взаимодействия, для эффективного участия в академических и профессиональных дискуссиях, различных научных мероприятиях, включая международные.
УК-5	Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	УК-5.1. Адекватно объясняет особенности поведения и мотивации людей различного социального и культурного происхождения в процессе взаимодействия с ними, опираясь на знания причин появления социальных обычаев и различий в поведении людей УК-5.2. Владеет навыками создания недискриминационной среды взаимодей-	*ПОРОГОВЫЙ («удовлетворительно»)*	*Выпускник знает:* - простейшие особенности протекания процессов межкультурного взаимодействия, поведения и мотивации людей различного социального и культурного происхождения; - некоторые базовые причины появления социальных обычаев и различий в поведении людей *Выпускник умеет:* - анализировать и учитывать на удовлетворительном уровне разнообразие культур в процессе межкультурного взаимодействия; - в удовлетворительной мере объяснить особенности поведения и мотивации людей различного социального и культурного происхождения в процессе взаимодействия с ними, опираясь на знания причин появления социальных обычаев и различий в поведении людей *Выпускник владеет:* - *базовыми* навыками межкультурного взаимодействия с людьми различного социального и культурного происхождения; - первичными навыками создания недискриминационной среды взаимодействия при выполнении профессиональных задач.
			БАЗОВЫ	*Выпускник знает:*

		ствия при выполнении профессиональных задач	*Й («хорошо»)*	- особенности протекания процессов межкультурного взаимодействия, поведения и мотивации людей различного социального и культурного происхождения; - причины появления социальных обычаев и различий в поведении людей *Выпускник умеет:* - анализировать и учитывать на достаточно глубоком уровне разнообразие культур в процессе межкультурного взаимодействия; - корректно и основательно объяснять особенности поведения и мотивации людей различного социального и культурного происхождения в процессе взаимодействия с ними, опираясь на знания причин появления социальных обычаев и различий в поведении людей *Выпускник владеет:* - хорошими навыками межкультурного взаимодействия с людьми различного социального и культурного происхождения; - навыками, достаточными для создания недискриминационной среды взаимодействия при выполнении профессиональных задач.
			ПОВЫШЕННЫЙ («отлично»)	*Выпускник знает:* - все основные особенности протекания процессов межкультурного взаимодействия, поведения и мотивации людей различного социального и культурного происхождения; - причины появления социальных обычаев и различий в поведении людей. *Выпускник умеет:* - глубоко и обстоятельно анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия; - грамотно и четко объяснить особенности поведения и мотивации людей различного социального и культурного происхождения в процессе взаимодействия с ними, опираясь на отличные знания причин появления социальных обычаев и различий в поведении людей *Выпускник владеет:* - эффективными навыками межкультурного взаимодействия с людьми различного социального и культурного происхождения; - эффективными навыками создания недискриминационной среды взаимодействия при выполнении профессиональных задач.
УК-6	Способен определять и реализовывать приори-	УК-6.1. Определяет приоритеты своей деятельности, выстраивает и реализовывает тра-	*ПОРОГОВЫЙ («удовлетворительно»)*	*Выпускник знает:* – возможные способы саморазвития в своей профессиональной деятельности. – основные направления развития науки и техники в профессиональной области деятельности. – приоритеты собственной деятельности и спо-

	теты собственной деятельности и способы ее совершенствования на основе самооценки	екторию саморазвития на основе мировоззренческих принципов УК-6.2. Использует личностный потенциал в социальной среде для достижения поставленный целей УК-6.3. Демонстрирует социальную ответственность за принимаемые решения, учитывает правовые и культурные аспекты, обеспечивает устойчивое развитие при ведении профессиональной и иной деятельности УК-6.4. Оценивает свою деятельность, соотносит цели, способы и средства выполнения деятельности с её результатами		собы её совершенствования с использованием нейронных сетей; - инструменты непрерывного образования и интеллектуальные справочные системы для выстраивания гибкой профессиональной траектории. – *Выпускник умеет:* – определять приоритеты своей деятельности, выстраивая и реализуя траекторию саморазвития на достижение результатов, направленных на профессиональную деятельность в сфере информационной безопасности. – определять приоритеты своей деятельности – планировать и решать задачи собственного профессионального и личностного развития; - реализовывать траектории саморазвития и самосовершенствования, применяя интеллектуальные обучающие системы. – *Выпускник владеет:* - базовыми навыками использования личностного потенциала на примере достижения поставленной цели научно-исследовательской работы в сфере информационной безопасности. - опытом использования личностного потенциала на примере достижения поставленной цели научно-исследовательской работы в сфере информационной безопасности – критическим анализом и оценками современных научных достижений; - навыками применения интеллектуальных алгоритмов поиска оптимальных решений для эффективного планирования и управления собственным временем.
			БАЗОВЫЙ («хорошо»)	*Выпускник знает:* – возможные способы саморазвития в своей профессиональной деятельности; – основные положения тайм-менеджмента. – основные направления развития науки и техники в профессиональной области деятельности, особенности развития на каждом этапе – приоритеты собственной деятельности и способы её совершенствования с использованием нейронных сетей; - инструменты непрерывного образования и интеллектуальные справочные системы для выстраивания гибкой профессиональной траектории; новые тренды в области разработки и использования систем искусственного интеллекта. –

				Выпускник умеет: – определять приоритеты своей деятельности, выстраивая и реализуя траекторию саморазвития на достижение результатов, направленных на профессиональную деятельность в сфере информационной безопасности. – определять приоритеты своей деятельности, выстраивая и реализуя траекторию саморазвития на достижение результатов – планировать и решать задачи собственного профессионального и личностного развития; – генерировать новые идеи при решении исследовательских и практических задач; - реализовывать траектории саморазвития и самосовершенствования, применяя интеллектуальные обучающие системы. – *Выпускник владеет:* - базовыми навыками использования личностного потенциала на примере достижения поставленной цели научно-исследовательской работы в сфере информационной безопасности - опытом использования личностного потенциала на примере достижения поставленной цели научно-исследовательской работы в сфере информационной безопасности – критическим анализом и оценками современных научных достижений; - навыками применения интеллектуальных алгоритмов и их программных реализаций для поиска оптимальных решений для эффективного планирования и управления собственным временем.
			ПОВЫШЕННЫЙ («отлично»)	*Выпускник знает:* – возможные способы саморазвития в своей профессиональной деятельности; – основные положения тайм-менеджмента; – требования работодателей к личностным и профессиональным качествам. – методологию научно-исследовательской деятельности в сфере информационной безопасности; – особенности диссертационного исследования как вида научно-исследовательской работы; – основные направления развития науки и техники в профессиональной области деятельности, особенности и закономерности развития на каждом этапе – приоритеты собственной деятельности и способы её совершенствования с использованием нейронных сетей; - инструменты непрерывного образования и

				интеллектуальные справочные системы для выстраивания гибкой профессиональной траектории; новые тренды в области разработки и использования систем искусственного интеллекта; принципы работы экспертных систем. – *Выпускник умеет:* – определять приоритеты своей деятельности, выстраивая и реализуя траекторию саморазвития на достижение результатов, направленных на профессиональную деятельность в сфере информационной безопасности; – планировать траекторию своей деятельности для развития личных и профессиональных качества. – определять приоритеты своей деятельности, выстраивая и реализуя траекторию саморазвития на достижение результатов, направленных на профессиональную деятельность в сфере информационной безопасности – планировать и решать задачи собственного профессионального и личностного развития; – генерировать новые идеи при решении исследовательских и практических задач; - реализовывать траектории саморазвития и самосовершенствования, применяя интеллектуальные обучающие системы; выполнять настройку необходимого окружения для работы с нейронными сетями. – *Выпускник владеет:* - опытом использования личностного потенциала на примере достижения поставленной цели научно-исследовательской работы в сфере информационной безопасности. - опытом использования личностного потенциала на примере достижения поставленной цели научно-исследовательской работы в сфере информационной безопасности – критическим анализом и оценками современных научных достижений; – правовыми и культурными аспектами в области истории развития искусственного интеллекта; - навыками применения интеллектуальных алгоритмов и их программных реализаций для поиска оптимальных решений для эффективного планирования и управления собственным временем; методологией разработки экспертных систем.
ОПК-1	Способен обосно-	ОПК-1.1. Анализирует систему обес-	*ПОРОГОВЫЙ («удовле-*	*Выпускник знает:* – основные требования, предъявляемые к системе обеспечения безопасности защищенных

	вывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	печения информационной безопасности и формулирует требования по ее улучшению. ОПК-1.2. Разрабатывает проект технического задания на создание системы обеспечения информационной безопасности.	*творительно»)*	информационных систем; – организационные и технические меры обеспечения информационной безопасности защищенных информационных систем; – уязвимости систем и угрозы безопасности информационных систем; – структуру технического задания и порядок его разработки и утверждения при проектировании защищенных информационных систем. *Выпускник умеет:* – формулировать требования к системе информационной безопасности; – разрабатывать к средствам и методам контроля проектируемой системы обеспечения информационной безопасности; – разрабатывать модели угроз и нарушителей информационной безопасности. *Выпускник владеет:* опытом разработки проекта технического задания на создание системы обеспечения информационной безопасности.
			БАЗОВЫЙ («хорошо»)	*Выпускник знает:* – основные требования, предъявляемые к системе обеспечения безопасности защищенных информационных систем; – организационные и технические меры обеспечения информационной безопасности защищенных информационных систем; – уязвимости систем и угрозы безопасности информационных систем; – структуру технического задания и порядок его разработки и утверждения при проектировании защищенных информационных систем; – структуру рабочего проекта и проектной документации, необходимых при разработке защищенных информационных систем. *Выпускник умеет:* – формулировать требования к системе информационной безопасности; – разрабатывать к средствам и методам контроля проектируемой системы обеспечения информационной безопасности; – проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты; – разрабатывать модели угроз и нарушителей информационной безопасности. *Выпускник владеет:* опытом разработки проекта технического задания на создание системы обеспечения информационной безопасности, подбора исходных данных.

			ПОВЫШЕННЫЙ («отлично»)	*Выпускник знает:* – основные требования, предъявляемые к системе обеспечения безопасности защищенных информационных систем; – организационные и технические меры обеспечения информационной безопасности защищенных информационных систем; – уязвимости систем и угрозы безопасности информационных систем; – структуру технического задания и порядок его разработки и утверждения при проектировании защищенных информационных систем; – структуру рабочего проекта и проектной документации, необходимых при разработке защищенных информационных систем; – нормативные документы, регламентирующие процесс разработки технических заданий по созданию систем обеспечения информационной безопасности объектов. *Выпускник умеет:* – формулировать требования к процессам и системам обеспечения информационной безопасности; – разрабатывать к средствам и методам контроля проектируемой системы обеспечения информационной безопасности; – проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты; – разрабатывать техническое задание на создание подсистем обеспечения информационной безопасности; – разрабатывать модели угроз и нарушителей информационной безопасности. *Выпускник владеет:* - опытом разработки проекта технического задания на создание системы обеспечения информационной безопасности, подбора исходных данных и моделирования процесса.
ОПК-2	Способен разрабатывать технический проект системы (подсистемы либо компонента	ОПК-2.1. Разрабатывает технический проект системы (подсистемы, компоненты системы) обеспечения информационной безопасности в соответствии с техническим заданием, нор-	*ПОРОГОВЫЙ («удовлетворительно»)*	*Выпускник знает:* – характеристики систем (подсистем либо компонентов системы) обеспечения информационной безопасности; – принципы организации и этапы разработки системы (подсистемы или компонента системы) обеспечения информационной безопасности; – средства тестирования системы (подсистемы или компонента системы) обеспечения информационной безопасности. *Выпускник умеет:* – формулировать требования к системам

	системы) обеспечения информационной безопасности	мативно-правовой, организационно-распорядительной и методической документацией.		обеспечения информационной безопасности; – осуществлять выбор подсистем, реализующих технологии обеспечения информационной безопасности; – осуществлять выбор подсистем, реализующих технологии обеспечения информационной безопасности; – разрабатывать планы и сценарии тестирования системы (подсистемы или компонента системы) обеспечения информационной безопасности. *Выпускник владеет:* - опытом разработки технического проекта системы (подсистемы либо компонента системы) обеспечения информационной безопасности
			БАЗОВЫЙ («хорошо»)	*Выпускник знает:* – характеристики систем, достоинства и недостатки (подсистем либо компонентов системы) обеспечения информационной безопасности; – технологии проектирования сложных систем; – принципы организации и этапы разработки системы (подсистемы или компонента системы) обеспечения информационной безопасности; – средства тестирования системы (подсистемы или компонента системы) обеспечения информационной безопасности. *Выпускник умеет:* – формулировать требования и параметры к системам обеспечения информационной безопасности; – осуществлять выбор подсистем, реализующих технологии обеспечения информационной безопасности; – разрабатывать планы и сценарии тестирования системы (подсистемы или компонента системы) обеспечения информационной безопасности; – разрабатывать технический проект системы обеспечения информационной безопасности. *Выпускник владеет:* - опытом разработки технического проекта системы (подсистемы либо компонента системы) обеспечения информационной безопасности, его моделирования
			ПОВЫШЕННЫЙ («отлично»)	*Выпускник знает:* – характеристики, параметры, достоинства и недостатки систем (подсистем либо компонентов системы) обеспечения информационной безопасности; – технологии проектирования сложных си-

				стем; – специализированное программное обеспечение в области проектирования сложных систем; – принципы организации и этапы разработки системы (подсистемы или компонента системы) обеспечения информационной безопасности; – средства тестирования системы (подсистемы или компонента системы) обеспечения информационной безопасности. *Выпускник умеет:* – формулировать требования, параметры к системам обеспечения информационной безопасности с учетом недостатков анализируемой системы; – осуществлять выбор подсистем, реализующих технологии обеспечения информационной безопасности; – разрабатывать планы и сценарии тестирования системы (подсистемы или компонента системы) обеспечения информационной безопасности; – разрабатывать и реализовывать технический проект системы обеспечения информационной безопасности. *Выпускник владеет:* - опытом разработки технического проекта системы (подсистемы либо компонента системы) обеспечения информационной безопасности, его моделирования и создания.
ОПК-3	Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности	ОПК-3.1. Разрабатывает проекты организационно-распорядительной документации, регламентирующих процесс обеспечения информационной безопасности	*ПОРОГОВЫЙ («удовлетворительно»)*	*Выпускник знает:* - порядок проведения испытаний средств и систем обеспечения информационной безопасности. - действующую нормативную документацию, регламентирующую порядок разработки и применения организационно-распорядительной документации в системе управления информационной безопасности *Выпускник умеет:* - проводить испытания средств и систем обеспечения информационной безопасности. - определять перечень организационно-распорядительной документации, необходимой для организации и реализации управления информационной безопасностью *Выпускник владеет:* - навыками применения методик и программ испытаний систем обеспечения информационной безопасности. - опытом разработки организационно-распорядительной документации по обеспече-

				нию деятельности в системе управления информационной безопасностью.
			БАЗОВЫЙ («хорошо»)	*Выпускник знает:* - порядок проведения испытаний средств и систем обеспечения информационной безопасности; - основные методы проведения испытания средств и систем обеспечения информационной безопасности. действующую нормативную документацию, регламентирующую порядок разработки и применения организационно-распорядительной документации, сроки ее утверждения и внесения изменений в системе управления информационной безопасности. *Выпускник умеет:* - проводить испытания средств и систем обеспечения информационной безопасности; - проводить анализ результатов проведенных испытаний систем обеспечения информационной безопасности. - определять перечень организационно-распорядительной документации, необходимой для организации и реализации управления информационной безопасностью *Выпускник владеет:* - навыками применения методик и программ испытаний систем обеспечения информационной безопасности. - опытом разработки и внедрения организационно-распорядительной документации по обеспечению деятельности в системе управления информационной безопасностью.
			ПОВЫШЕННЫЙ («отлично»)	*Выпускник знает:* - порядок проведения испытаний средств и систем обеспечения информационной безопасности; - основные методы и программы проведения испытания средств и систем обеспечения информационной безопасности. – действующую нормативную документацию, регламентирующую порядок разработки и применения организационно-распорядительной документации, сроки ее утверждения и внесения изменений, особенности внесенных изменений в системе управления информационной безопасности. *Выпускник умеет:* - проводить испытания средств и систем обеспечения информационной безопасности; - проводить анализ результатов проведенных испытаний средств и систем обеспечения информационной безопасности.

				– определять перечень организационно-распорядительной документации, необходимой для организации и реализации управления информационной безопасностью. *Выпускник владеет:* - навыками применения методик и программ испытаний средств и систем обеспечения информационной безопасности. - опытом разработки и внедрения организационно-распорядительной документации по обеспечению информационной безопасности, анализу результатов внедрения документации и принятию корректирующих мер по обеспечению деятельности в системе управления информационной безопасностью.
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-4.1. Осуществляет поиск научно-технической информации для решения поставленной задачи, обработку и анализ собранных данных. ОПК-4.2. Осуществляет планирование эксперимента, разрабатывает программу проведения исследований.	*ПОРОГОВЫЙ («удовлетворительно»)*	*Выпускник знает:* - перечень научно-технической информации, необходимой для достижения поставленной цели. *Выпускник умеет:* - собирать собранную информацию для решения поставленной задачи. *Выпускник владеет:* - *опытом анализа научно-технической информации.*
			БАЗОВЫЙ («хорошо»)	*Выпускник знает:* - перечень научно-технической информации, необходимой для достижения поставленной цели; - порядок сбора необходимой научно-технической информации; - специфику управления научно-исследовательскими работами в вузе. *Выпускник умеет:* - собирать и анализировать собранную информацию для решения поставленной задачи; - эффективно работать с современными печатными и электронными источниками научной информации. *Выпускник владеет:* - *опытом анализа научно-технической информации;* - *-опытом планирования эксперимента для решения поставленной задачи.*
			ПОВЫШЕННЫЙ («отлично»)	*Выпускник знает:* - перечень научно-технической информации, необходимой для достижения поставленной цели; - порядок сбора необходимой научно-технической информации; - порядок планирования эксперимента для решения поставленной задачи; - специфику управления научно-

				исследовательскими работами в вузе; - процедуру подготовки и защиты диссертационного исследования. *Выпускник умеет:* - собирать и анализировать собранную информацию для решения поставленной задачи; - эффективно работать с современными печатными и электронными источниками научной информации. *Выпускник владеет:* *- опытом анализа научно-технической информации;* *- -опытом планирования эксперимента для решения поставленной задачи;* *- опытом применения статистических методов при планировании эксперимента.*
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.	ОПК-5.1. Проводит исследования в соответствии с разработанным планом и программой. ОПК-5.2. Обрабатывает полученные результаты с применением методом математической статистики. ОПК-5.3. Осуществляет подготовку научно-технических отчетов, аналитических обзоров, научных докладов и статей.	*ПОРОГОВЫЙ («удовлетворительно»)*	*Выпускник знает:* – методы проведения научных исследований и обработки результатов. *Выпускник умеет:* – проводить математическую обработку полученных результатов. *Выпускник владеет:* опытом составления научно-технических отчетов по результатам проведенных исследований.
			БАЗОВЫЙ («хорошо»)	*Выпускник знает:* – методы проведения научных исследований и обработки результатов; – алгоритм обработки полученных результатов. *Выпускник умеет:* – проводить математическую обработку полученных результатов. *Выпускник владеет:* опытом составления научно-технических отчетов по результатам проведенных исследований, анализа полученных результатов.
			ПОВЫШЕННЫЙ («отлично»)	*Выпускник знает:* – методы проведения научных исследований и обработки результатов; – алгоритм обработки и анализа полученных результатов; – обрабатывать аналитическую информацию в области научных разработок *Выпускник умеет:* – проводить математическую обработку полученных результатов. *Выпускник владеет:* - опытом составления научно-технических отчетов по результатам проведенных исследований, анализа полученных результатов и фор-

				мировки выводов; - опытом использования специализированного программного обеспечения в области аналитически больших данных.
ПК-1	ПК-1 Способен выявлять основные тенденции развития в области информационной безопасности, прогнозировать потенциальные угрозы и риски в работе информационно-аналитических систем, осуществлять построение и применение систем и средств защиты информации	ПК-1.1 Характеризует по назначению и классификационным характеристикам информационные и аналитические системы. ПК-1.2 Осуществляет функционирование процесса обеспечения безопасности информационно-аналитических систем; выявляет, классифицирует и оценивает уязвимости информационно-аналитических систем, угрозы и риски безопасности. ПК-1.3 Определяет требования к техническим и программным средствам защиты информации в информационно-аналитических системах, проводит обоснование характеристик и функциональных возможностей средств обеспечения информационной безопасности информацион-	*ПОРОГОВЫЙ («удовлетворительно»)*	*Выпускник знает:* - методы, способы и принципы построения защищенных информационно-аналитических систем; - порядок проектирования защищенных информационно-аналитических систем; - классификацию защищенных информационно-аналитических систем; - основные понятия по аттестации объектов информатизации; - требования к объектам информатизации для последующей аттестации; - понятие об информационно-аналитических и экспертных системах, их назначение; - классификацию, характеристики и порядок выявления угроз безопасности; - требования, предъявляемые к информационно-аналитическим системам. - требования, предъявляемые к информационно-аналитическим системам по обеспечению их безопасности; - физические методы, лежащие в основе применения технологий обеспечения информационной безопасности; - средства и способы обеспечения информационной безопасности; - принципы построения систем защиты информации; - характеристики технологий и средств защиты по обеспечению информационной безопасности; - нормативные правовые акты, руководящие и методические документы уполномоченных федеральных органов исполнительной власти в области защиты информации - основные риски безопасности информационно-аналитических систем. - категорийный и понятийный аппарат в области защищенности информации от несанкционированного доступа; - методы и технологии контроля защищенности информации от несанкционированного доступа; - методы экспериментальных исследований для выявления фактов несанкционированного доступа. - категорийный и понятийный аппарат в области защищенности информации от несанкционированного доступа по техническим каналам; - методы и технологии контроля защищенно-

		но-аналитических систем. ПК-1.4 Осуществляет подбор и применение средств и способов обеспечения информационной безопасности при построении системы защиты в информационно-аналитических системах, проводит оценку эффективности реализации системы защиты информации. ПК 1.5 Осуществляет применение организационных мер защиты информации.		сти информации от несанкционированного доступа; - методы экспериментальных исследований для выявления технических каналов от утечки информации. *Выпускник умеет:* - составлять техническое предложение на разработку защищенных информационно-аналитических систем; - разрабатывать общие решения по системе и ее частям, функционально-алгоритмическую структуру системы; - применять аттестованные объекты информатизации; - выявлять объекты и угрозы безопасности информационно-аналитических систем, прогнозировать последствия реализации этих угроз; - осуществлять построение модели угроз и модели нарушителей. - выявлять объекты и угрозы безопасности автоматизированных систем, прогнозировать последствия реализации этих угроз; - применять средства, обеспечивающие защиту информации. - анализировать возможные уязвимости информационно-аналитических систем. - выявлять уязвимости компонентов объекта исследования; - определять уровень защищенности объекта исследования; - разрабатывать системы для контроля защищенности информации от несанкционированного доступа; - проводить исследования по выявлению каналов несанкционированного доступа; - анализировать результаты процесса оценки уровня защищенности. - выявлять уязвимости компонентов объекта исследования от утечки по техническим каналам; - разрабатывать системы для контроля защищенности информации от утечки; - проводить исследования по выявлению каналов утечки информации и защиты от нее. *Выпускник владеет:* - навыками обоснования требуемых характеристик защищенных информационно-аналитических систем; - опытом планирования процесса проектирова-

				ния защищенных информационно-аналитических систем; - навыками организации мероприятий по защите информации на объекте информатизации; - навыками представления знаний, правил их вывода и обработки с использованием логической и продукционной моделей; - навыками выявления угроз безопасности информационно-аналитических и экспертных систем; - навыками обеспечения безопасности информационно-аналитических и экспертных систем; - навыками применения технологий обеспечения безопасности информационно-аналитических систем. - навыком и опытом оценки затрат и рисков при использовании информационных технологий, формирования политики безопасности объектов защиты учетом специфики этих объектов; - навыками систематизации результатов проведенных исследований; - навыками систематизации рисков информационной безопасности. - навыками подготовки мотивированного заключения по оценке состояния защищенности информационно-аналитической системы; - навыками применения специальных технических средств для защиты информации от несанкционированного доступа; - навыками применения средств обработки результатов исследований по защите от несанкционированного доступа; - навыками описания выявленных уязвимостей, ранжирования их по степени потенциальной опасности, вероятности их использования, типу злоумышленника; описания последствий реализации выявленных уязвимостей. - навыками подготовки мотивированного заключения по оценке состояния защищенности информационно-аналитической системы от утечки по техническим каналам; - навыками применения специальных технических средств для защиты информации от утечки по техническим каналам; - навыками применения средств обработки результатов исследований по выявлению каналов утечки информации.
			БАЗОВЫЙ	*Выпускник знает:* - методы, способы и принципы построения за-

			(«хорошо»)	щищенных информационно-аналитических систем; - порядок проектирования защищенных информационно-аналитических систем; - классификацию защищенных информационно-аналитических систем; - основные понятия по аттестации объектов информатизации; - требования к объектам информатизации для последующей аттестации; - порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа; - понятие об информационно-аналитических и экспертных системах, их назначение, характеристики и классификацию; - классификацию, характеристики и порядок выявления угроз безопасности; - требования, предъявляемые к информационно-аналитическим системам. - требования, предъявляемые к информационно-аналитическим системам по обеспечению их безопасности; - физические методы, лежащие в основе применения технологий обеспечения информационной безопасности; - средства и способы обеспечения информационной безопасности; - принципы построения систем защиты информации; - характеристики технологий и средств защиты по обеспечению информационной безопасности; - методы обработки результатов, касающихся применения технологий обеспечения информационной безопасности; - нормативные правовые акты, руководящие и методические документы уполномоченных федеральных органов исполнительной власти в области защиты информации. - основные риски безопасности информационно-аналитических систем; - подходы к построению моделей процессов защиты информации в информационно-аналитических системах. - категорийный и понятийный аппарат в области защищенности информации от несанкционированного доступа; - классификацию и характеристики показателей защищенности информации от несанкционированного доступа; - методы и технологии контроля защищенности информации от несанкционированного до-

				ступа; - методы экспериментальных исследований для выявления фактов несанкционированного доступа к информации. - категорийный и понятийный аппарат в области защищенности информации от несанкционированного доступа по техническим каналам; - методы и технологии контроля защищенности информации от несанкционированного доступа; - методы экспериментальных исследований для выявления технических каналов от утечки информации; - классификацию и характеристики показателей защищенности информации от несанкционированного доступа по техническим каналам. *Выпускник умеет:* - составлять техническое предложение на разработку информационно-аналитических систем; - разрабатывать общие решения по системе и ее частям, функционально-алгоритмическую структуру системы, алгоритмы решения задач и применяемые языки, систему классификации и кодирования информации; - применять аттестованные объекты информатизации; - проводить аттестационные испытания; - выявлять объекты и угрозы безопасности информационно-аналитических систем, прогнозировать последствия реализации этих угроз; - осуществлять построение модели угроз и модели нарушителей; - формулировать требования, обеспечивающие безопасность информации информационно-аналитических систем. - выявлять объекты и угрозы безопасности автоматизированных систем, прогнозировать последствия реализации этих угроз; - разрабатывать модели нарушителей и угроз; - применять средства и технологии, обеспечивающие защиту информации. - анализировать возможные уязвимости информационно-аналитических систем; - выявлять возможные риски, связанные с обработкой информации в информационных системах. - выявлять уязвимости компонентов объекта исследования; - определять уровень защищенности объекта исследования; - разрабатывать системы для контроля защи-

				щенности информации от несанкционированного доступа; - проводить исследования по защите от несанкционированного доступа; - анализировать результаты процесса оценки уровня защищенности. - выявлять уязвимости компонентов объекта исследования от утечки по техническим каналам; - разрабатывать системы для контроля защищенности информации от утечки; - проводить исследования по выявлению каналов утечки информации и защиты от нее; - определять уровень защищенности объекта исследования. *Выпускник владеет:* - навыками обоснования требуемых характеристик защищенных информационно-аналитических систем; - опытом планирования процесса проектирования защищенных информационно-аналитических систем; - навыками организации мероприятий по защите информации на объекте информатизации; - навыками представления знаний, правил их вывода и обработки с использованием логической и продукционной моделей; - навыками представления знаний в виде семантической сети; - навыками выявления угроз безопасности информационно-аналитических и экспертных систем; - навыками обеспечения безопасности информационно-аналитических и экспертных систем. - навыками применения технологий обеспечения безопасности информационно-аналитических систем; - навыками применения технических и программных средств защиты информации в информационно-аналитических системах. - навыком и опытом оценки затрат и рисков при использовании информационных технологий, формирования политики безопасности объектов защиты учетом специфики этих объектов; - навыками систематизации результатов проведенных исследований; - навыками систематизации, оценки и обработки рисков информационной безопасности. - навыками подготовки мотивированного заключения по оценке состояния защищенности

				информационно-аналитической системы; - навыками применения специальных технических средств для защиты информации от несанкционированного доступа; - навыками применения средств обработки результатов исследований при защите от несанкционированного доступа; - навыками описания выявленных уязвимостей, ранжирования их по степени потенциальной опасности, вероятности их использования, типу злоумышленника; описания последствий реализации выявленных уязвимостей. - навыками подготовки мотивированного заключения по оценке состояния защищенности информационно-аналитической системы от утечки по техническим каналам; - навыками применения специальных технических средств для защиты информации от утечки по техническим каналам; - навыками применения средств обработки результатов исследований по выявлению каналов утечки информации; - навыками описания выявленных уязвимостей, ранжирования их по степени потенциальной опасности, вероятности их использования, типу злоумышленника; описания последствий реализации выявленных уязвимостей.
			ПОВЫШЕННЫЙ («отлично»)	*Выпускник знает:* - методы, способы и принципы построения защищенных информационно-аналитических систем; - порядок проектирования защищенных информационно-аналитических систем; - классификацию, характеристики защищенных информационно-аналитических систем; - основные понятия по аттестации объектов информатизации; - требования к объектам информатизации для последующей аттестации; - порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа; - состав и содержание этапов работ по внедрению и вводу в эксплуатацию систем защиты информации объектов информатизации; - понятие об информационно-аналитических и экспертных системах, их назначение, характеристики и классификацию; - архитектуру и технологии разработки экспертных систем; - классификацию, характеристики и порядок

				выявления угроз безопасности; - требования, предъявляемые к информационно-аналитическим системам. - требования, предъявляемые к информационно-аналитическим системам по обеспечению их безопасности; - физические методы, лежащие в основе применения технологий обеспечения информационной безопасности; - средства и способы обеспечения информационной безопасности; - принципы построения систем защиты информации; - характеристики технологий и средств защиты по обеспечению информационной безопасности; - методы обработки результатов, касающихся применения технологий обеспечения информационной безопасности; - характеристики технических и программных средств, применяемых для обеспечения безопасности ИАС; - нормативные правовые акты, руководящие и методические документы уполномоченных федеральных органов исполнительной власти в области защиты информации. - основные риски безопасности информационно-аналитических систем; - подходы к построению и исследованию моделей процессов защиты информации в информационно-аналитических системах. - категорийный и понятийный аппарат в области защищенности информации от несанкционированного доступа; - классификацию и характеристики показателей защищенности информации от несанкционированного доступа; - методы и технологии контроля защищенности информации от несанкционированного доступа; - методы экспериментальных исследований для выявления фактов несанкционированного доступа к информации; - методы и способы защиты информации от несанкционированного доступа. - категорийный и понятийный аппарат в области защищенности информации от утечки по техническим каналам; - классификацию и характеристики показателей защищенности информации от утечки по техническим каналам; - методы и технологии контроля защищенности информации от несанкционированного доступа;

				- методы экспериментальных исследований для выявления технических каналов от утечки информации; - методы и способы защиты информации от несанкционированного доступа по техническим каналам. *Выпускник умеет:* - составлять техническое предложение на разработку защищенных информационно-аналитических систем; - разрабатывать общие решения по системе и ее частям, функционально-алгоритмическую структуру системы, функции персонала и организационную структуру, алгоритмы решения задач и применяемые языки, систему классификации и кодирования информации, программное обеспечение; - применять аттестованные объекты информатизации; - проводить аттестационные испытания; - характеризовать модели представления знаний; - выявлять объекты и угрозы безопасности информационно-аналитических систем, прогнозировать последствия реализации этих угроз; - осуществлять построение модели угроз и модели нарушителей; - формулировать требования, обеспечивающие безопасность информации информационно-аналитических систем. - выявлять объекты и угрозы безопасности автоматизированных систем, прогнозировать последствия реализации этих угроз; - разрабатывать модели нарушителей и угроз; - применять средства и технологии, обеспечивающие защиту информации; - обрабатывать результаты эксперимента по применению технологий обеспечения информационной безопасности. - анализировать возможные уязвимости информационно-аналитических систем; - выявлять возможные риски, связанные с обработкой информации в информационных системах; - разрабатывать модели оценки рисков и доказывать адекватность данных моделей для использования в системе защиты информации. - выявлять уязвимости компонентов объекта исследования; - определять уровень защищенности объекта исследования;

				- разрабатывать системы для контроля от несанкционированного доступа; - проводить исследования по выявлению каналов от несанкционированного доступа; - анализировать результаты процесса оценки уровня защищенности и осуществлять модификацию уровня защищенности информации в информационно-аналитических системах. - выявлять уязвимости компонентов объекта исследования от утечки по техническим каналам; - определять уровень защищенности объекта исследования; - разрабатывать системы для контроля защищенности информации от утечки; - проводить исследования по выявлению каналов утечки информации и защиты от нее; - анализировать результаты процесса оценки уровня защищенности информации от утечки по техническим каналам и осуществлять модификацию уровня защищенности информации в информационно-аналитических системах. *Выпускник владеет:* - навыками обоснования требуемых характеристик защищенных информационно-аналитических систем; - опытом планирования процесса проектирования защищенных информационно-аналитических систем; - навыками организации мероприятий по защите информации на объекте информатизации; - навыками представления знаний, правил их вывода и обработки с использованием логической и продукционной моделей; - навыками представления знаний в виде семантической сети; - навыками применения нечеткой логики в экспертных системах; - навыками выявления угроз безопасности информационно-аналитических и экспертных систем; - навыками обеспечения безопасности информационно-аналитических и экспертных систем. - навыками применения технологий обеспечения безопасности информационно-аналитических систем; - навыками применения технических и программных средств защиты информации в информационно-аналитических системах; - навыками проведения сравнительной харак-

				теристики средств защиты информации в информационно-аналитических системах. - навыком и опытом оценки затрат и рисков при использовании информационных технологий, формирования политики безопасности объектов защиты учетом специфики этих объектов; - навыками систематизации результатов проведенных исследований; - навыками систематизации, оценки и обработки рисков информационной безопасности; - навыками применения программного обеспечения для оценки обработки рисков в задачах моделирования и исследования моделей систем защиты информации. - навыками подготовки мотивированного заключения по оценке состояния защищенности информационно-аналитической системы; - навыками описания выявленных уязвимостей, ранжирования их по степени потенциальной опасности, вероятности их использования, типу злоумышленника; описания последствий реализации выявленных уязвимостей; - навыками применения специальных технических средств для защиты информации от несанкционированного доступа; - навыками применения средств обработки результатов исследований при защите от несанкционированного доступа; - навыками подготовки рекомендаций по нейтрализации выявленных уязвимостей (снижению возможного ущерба от их использования злоумышленниками), рекомендаций по изменению конфигурации и настроек оборудования, используемых защитных механизмов и программных средств, принятию дополнительных мер и применению дополнительных средств защиты, по установке необходимых обновлений для используемого программного обеспечения и т.п. - навыками подготовки мотивированного заключения по оценке состояния защищенности информационно-аналитической системы от утечки по техническим каналам; - навыками применения специальных технических средств для защиты информации от утечки по техническим каналам; - навыками применения средств обработки результатов исследований по выявлению каналов утечки информации; - навыками описания выявленных уязвимостей, ранжирования их по степени потенциальной опасности, вероятности их использования, типу злоумышленника; описания послед-

				ствий реализации выявленных уязвимостей; - навыками подготовки рекомендаций по нейтрализации выявленных уязвимостей (снижению возможного ущерба от их использования злоумышленниками), рекомендаций по изменению конфигурации и настроек оборудования, используемых защитных механизмов и программных средств, принятию дополнительных мер и применению дополнительных средств защиты, по установке необходимых обновлений для используемого программного обеспечения и т.п.
ПК-2	ПК-2 Способен проводить исследования, обрабатывать и анализировать полученные результаты	ПК-2.1 Осуществляет поиск и анализ научно-технической информации, выбор технологий, методов и способов решения профессиональных задач, разрабатывает планы проведения научных исследований. ПК-2.2 Обрабатывает полученные результаты, оформляет научно-технические отчеты, готовит обзоры, научные статьи и доклады.	*ПОРОГОВЫЙ («удовлетворительно»)*	*Выпускник знает:* - порядок проведения научных исследований в рамках выполнения магистерской диссертации; - способы представления результатов научных исследований (охранные документы, тезисы докладов конференций, статьи). - объекты и субъекты права интеллектуальной собственности; - основные понятия о патентной информации и документации. *Выпускник умеет:* - формулировать цель, задачи проведения научных исследований для решения поставленных проблем; - проводить сравнительный анализ нормативно-методической и научной литературы для решения поставленных задач. - использовать знания, полученные в процессе обучения в университете, для оформления прав на объекты интеллектуальной собственности; - применять некоторые варианты расчета экономической эффективности внедрения объектов интеллектуальной собственности; - применять знания поиска патентной информации во время выполнения курсовых и дипломных проектов. *Выпускник владеет:* - навыками проведения библиографического поиска информации по заданной теме с применением современных информационных технологий; - навыками подготовки тезисов докладов конференций и научной статьи в области информационной безопасности. - навыками работы с научной и справочной литературой.

			БАЗОВЫЙ («хорошо»)	*Выпускник знает:* - принципы проведения библиографической работы с применением современных информационных технологий; - порядок проведения научных исследований в рамках выполнения магистерской диссертации; - способы представления результатов научных исследований (охранные документы, тезисы докладов конференций, статьи). - объекты и субъекты права интеллектуальной собственности; - способы защиты прав; авторов и владельцев объектов интеллектуальной собственности; - основные понятия о патентной информации и документации. *Выпускник умеет:* - формулировать проблемы по обеспечению безопасности информационной-аналитических систем, применяемых технических и программных средств защиты информации; - формулировать цель, задачи проведения научных исследований для решения поставленных проблем; - проводить сравнительный анализ нормативно-методической и научной литературы для решения поставленных задач. - использовать знания, полученные в процессе обучения в университете, для оформления прав на объекты интеллектуальной собственности; - применять некоторые варианты расчета экономической эффективности внедрения объектов интеллектуальной собственности; - применять знания поиска патентной информации во время выполнения курсовых и дипломных проектов; - исследовать и правильно формулировать признаки новизны в разрабатываемых объектах. *Выпускник владеет:* - навыками планирования эксперимента; - навыками проведения библиографического поиска информации по заданной теме с применением современных информационных технологий; - навыками подготовки тезисов докладов конференций и научной статьи в области информационной безопасности. - основными способами и навыками решения практических задач; - навыками работы с научной и справочной литературой.

			ПОВЫШЕННЫЙ («отлично»)	*Выпускник знает:* - принципы проведения библиографической работы с применением современных информационных технологий; - порядок проведения научных исследований в рамках выполнения магистерской диссертации; - способы представления результатов научных исследований (охранные документы, тезисы докладов конференций, статьи), правила их подготовки и представления. - объекты и субъекты права интеллектуальной собственности; - права и обязанности авторов и владельцев объектов интеллектуальной собственности; - способы защиты прав; авторов и владельцев объектов интеллектуальной собственности; - основные понятия о патентной информации и документации. *Выпускник умеет:* - формулировать проблемы по обеспечению безопасности информационной-аналитических систем, применяемых технических и программных средств защиты информации; - формулировать цель, задачи проведения научных исследований для решения поставленных проблем; - проводить сравнительный анализ нормативно-методической и научной литературы для решения поставленных задач; - проводить критический анализ результатов проведенных исследований. - использовать знания, полученные в процессе обучения в университете, для оформления прав на объекты интеллектуальной собственности; - применять некоторые варианты расчета экономической эффективности внедрения объектов интеллектуальной собственности; - применять знания поиска патентной информации во время выполнения курсовых и дипломных проектов; - исследовать и правильно формулировать признаки новизны в разрабатываемых объектах; - правильно оформить заявку на изобретение, полезную модель, промышленный образец. *Выпускник владеет:* - навыками планирования эксперимента; - навыками проведения библиографического поиска информации по заданной теме с применением современных информационных технологий;

				- навыками подготовки охранного документа, тезисов докладов конференций и научной статьи в области информационной безопасности. - основными способами и навыками решения практических задач; - навыками работы с научной и справочной литературой; - методикой работы с методическими и нормативными материалами, техническими условиями и стандартами технологического проектирования.
ПК-3	ПК-3 Способен организовать работу по созданию, эксплуатации и модернизации информационно-аналитических систем и средств защиты в информационно-аналитических системах	ПК-3.1 Организует выполнение работ и управляет работой коллектива по эксплуатации, созданию и модернизации информационно-аналитических систем и средств защиты в информационно-аналитических системах. ПК-3.2 Применяет системы управления с учетом назначения классификационных характеристик информационных и аналитических систем. ПК-3.3 Принимает управленческие решения и оценивает их эффективность для обеспечения безопасности информационно-аналитических систем в соответствии с требованиями	*ПОРОГОВЫЙ («удовлетворительно»)*	*Выпускник знает:* - принципы и методы применения системного, структурного анализа при проектировании и эксплуатации информационно-аналитических систем и средств защиты; - содержание нормативных документов, регламентирующих процесс управления рисками. - основные функции управления применительно к информационной безопасности; - научные основы и цели управленческой деятельности; - основные методы и алгоритм принятия управленческих решений; - основные функции управления; - научные основы и цели управленческой деятельности. - порядок процесса создания информационно-аналитических систем; - базовые принципы организации работы в информационно-аналитическом подразделения. - порядок процесса создания информационных систем на разных этапах жизненного цикла. - основные способы получения и анализа информации для реализации функций стратегического менеджмента. *Выпускник умеет:* - применять основы структурного анализа при эксплуатации и проектировании информационно-аналитических систем и технических средств - применять нормативные правовые акты, регламентирующие процесс управления рисками. - организовывать работы по управлению информационной безопасностью. - применять алгоритм разработки управленческих решений в управлении информационной безопасностью; - организовывать работы по управлению информационной безопасностью. - осуществлять модернизацию информацион-

		нормативной правовой и организационно-методической документации.		но-аналитических систем; - организовывать работу информационно-аналитического подразделения. - осуществлять модернизацию информационных систем на стадии зрелости жизненного цикла. - ставить цели (SMART) и формулировать задачи, связанные с реализацией профессиональных функций. *Выпускник владеет:* - навыками обоснования характеристик средств обеспечения информационной безопасности на основе системного подхода; - навыками организации и управления работой специалистов в процессе управления рисками. - методикой формирования команды и организации работы по управлению информационной безопасностью. - методикой формирования команды и организации работы по управлению информационной безопасностью; методикой оценки эффективности принятых управленческих решений. - опытом организации работ по созданию и эксплуатации информационной безопасности защищаемого объекта. - опытом организации работ по созданию и эксплуатации информационной безопасности защищаемого объекта на разных этапах жизненного цикла; - опытом управления работой коллектива работников на разных этапах жизненного цикла информационно-аналитических систем. - культурой стратегического мышления, навыками постановки целей и выбора способов их достижения.
			БАЗОВЫЙ («хорошо»)	*Выпускник знает:* - принципы и методы применения системного, структурного анализа при проектировании и эксплуатации информационно-аналитических систем и средств защиты; - методологию применения системного анализа сложных систем управления; - основные подходы организации процесса управления рисками; - содержание нормативных документов, регламентирующих процесс управления рисками. - основные функции управления применительно к информационной безопасности; - способы организации работ по управлению

				информационной безопасностью с позиции процессного подхода; - научные основы, цели и принципы управленческой деятельности. - основные методы и алгоритм принятия управленческих решений; - особенности принятия управленческих решений в управлении информационной безопасностью; - основные функции управления применительно к информационной безопасности; - научные основы, цели и принципы управленческой деятельности. - порядок процесса создания и эксплуатации информационно-аналитических систем; - принципы организации работы в информационно-аналитическом подразделения; - принципы организации работы специалистов по созданию и эксплуатации средств защиты в информационно-аналитической системе. - порядок процесса создания и эксплуатации информационных систем на разных этапах жизненного цикла; - принципы организации работы в информационно-аналитическом подразделения. - основные способы получения и анализа информации для реализации функций стратегического менеджмента; - основы стратегического управления для разработки и реализации концепции управления персоналом. *Выпускник умеет:* - применять основы структурного анализа при эксплуатации и проектировании информационно-аналитических систем и технических средств; - применять системные принципы при эксплуатации и проектировании систем защиты информации; - применять нормативные правовые акты, регламентирующие процесс управления рисками; - проводить аудит информационной безопасности и принимать управленческие решения в процессе управления рисками. - организовывать работы по управлению информационной безопасностью на основе принципов процессного подхода. - организовывать работы по управлению информационной безопасностью на основе принципов процессного подхода; - применять алгоритм разработки управленче-

				ских решений в управлении информационной безопасностью. - осуществлять модернизацию информационно-аналитических систем; - организовывать работу информационно-аналитического подразделения; - организовывать процессы создания информационно-аналитической системы. - осуществлять модернизацию информационных систем на стадии зрелости жизненного цикла; - опытом управления работой коллектива работников на разных этапах жизненного цикла информационно-аналитических систем; - организовывать процессы создания информационно-аналитической системы; - разрабатывать проекты методических документов, регламентирующих функционирование ИАС. - ставить цели (SMART) и формулировать задачи, связанные с реализацией профессиональных функций. *Выпускник владеет:* - навыками обоснования характеристик средств обеспечения информационной безопасности на основе системного подхода; - опытом планирования процесса проектирования информационно-аналитических систем на основе системного подхода; - навыками организации и управления работой специалистов в процессе управления рисками; - навыками применения процессного подхода в организации процедуры управлении рисками информационной безопасности. - методикой формирования команды и организации работы по управлению информационной безопасностью на основе принципов процессного подхода - методикой формирования команды и организации работы по управлению информационной безопасностью; - методикой оценки эффективности принятых управленческих решений в вопросах информационной безопасности. - опытом организации работ по созданию и эксплуатации информационной безопасности защищаемого объекта; - навыками разработки методических документов, регламентирующих функционирование ИАС. - опытом организации работ по созданию и эксплуатации информационной безопасности

				защищаемого объекта. - культурой стратегического мышления, навыками постановки целей и выбора способов их достижения; - навыками разработки и реализации стратегии организации.
			ПОВЫШЕННЫЙ («отлично»)	*Выпускник знает:* - принципы и методы применения системного, структурного анализа при проектировании и эксплуатации информационно-аналитических систем и средств защиты; - методологию применения системного анализа сложных систем управления; - научные основы, цели, задачи, принципы, методы и технологии управленческой деятельности; - основные подходы, методы и технологии организации процесса управления рисками; - содержание нормативных документов, регламентирующих процесс управления рисками. - основные функции управления применительно к информационной безопасности; - способы организации работ по управлению информационной безопасностью с позиции процессного подхода; - стандарты в области информационной безопасности; - особенности использования процессного подхода при построении системы управления информационной безопасностью; - научные основы, цели, принципы, методы и технологии управленческой деятельности - основные методы и алгоритм принятия управленческих решений; - особенности принятия управленческих решений в управлении информационной безопасностью; - основные функции управления применительно к информационной безопасности; - способы организации работ по управлению информационной безопасностью с позиции процессного подхода; - стандарты в области информационной безопасности; - научные основы, цели, принципы, методы и технологии управленческой деятельности. - порядок процесса создания, эксплуатации и модернизации информационно-аналитических систем; - принципы и методы организации работы в информационно-аналитическом подразделения; - принципы и методы организации работы спе-

				циалистов по созданию и эксплуатации средств защиты в информационно-аналитической системе; - организационные меры по защите информации. - порядок процесса создания, эксплуатации и модернизации информационных систем на разных этапах жизненного цикла; - принципы и методы организации работы в информационных подразделениях; - принципы и методы организации работы специалистов по созданию и эксплуатации средств защиты в информационно-аналитической системе; - организационные меры по защите информации. - основные способы получения и анализа информации для реализации функций стратегического менеджмента; - основы стратегического управления для разработки и реализации концепции управления персоналом; - взаимосвязь стратегии организации и стратегии управления персоналом. *Выпускник умеет:* - применять основы структурного анализа при эксплуатации и проектировании информационно-аналитических систем и технических средств; - применять системные принципы при эксплуатации и проектировании систем защиты информации; - принимать управленческие решения и оценивать их эффективность; - разрабатывать стратегию процесса управления рисками; - применять нормативные правовые акты, регламентирующие процесс управления рисками; - проводить аудит информационной безопасности и принимать управленческие решения в процессе управления рисками. - организовывать работы по управлению информационной безопасностью на основе принципов процессного подхода; - использовать принципы организации системы управления информационной безопасностью на основе процессного подхода. - организовывать работы по управлению информационной безопасностью; - использовать принципы организации систе-

				мы управления информационной безопасностью - применять алгоритм разработки управленческих решений в управлении информационной безопасностью; - использовать принципы принятия управленческих решений в управлении информационной безопасностью. - организовывать работу информационно-аналитического подразделения; - организовывать процессы создания и эксплуатации информационно-аналитической системы; - разрабатывать проекты методических и организационно-распорядительных документов, регламентирующих функционирование ИАС. - осуществлять модернизацию информационных систем на разных этапах жизненного цикла; - опытом управления работой коллектива работников на разных этапах жизненного цикла информационных систем - организовывать процессы создания и эксплуатации информационно-аналитической системы; - разрабатывать проекты методических документов, регламентирующих функционирование ИАС. - ставить цели (SMART) и формулировать задачи, связанные с реализацией профессиональных функций; - применять инструменты стратегического менеджмента для формирования трудового потенциала организации и достижения организационных целей. *Выпускник владеет:* - навыками обоснования характеристик средств обеспечения информационной безопасности на основе системного подхода; - опытом планирования процесса проектирования информационно-аналитических систем на основе системного подхода; - опытом представления информации в систематизированном виде, оформления научно-технического отчета или материала для выступления или публикации; - навыками организации и управления работой специалистов в процессе управления рисками; - навыками применения процессного подхода в организации процедуры управлении рисками информационной безопасности; - навыками документального сопровождения

				организации процесса управления рисками. - методикой формирования команды и организации работы по управлению информационной безопасностью на основе принципов процессного подхода; - методикой использования процессного подхода при формировании системы управления информационной безопасностью - методикой формирования команды и организации работы по управлению информационной безопасностью на основе принципов процессного подхода; - методикой использования процессного подхода при формировании системы управления информационной безопасностью; - методикой оценки эффективности принятых управленческих решений в вопросах информационной безопасности. - опытом организации работ по созданию и эксплуатации информационной безопасности защищаемого объекта; - навыками разработки методических документов, регламентирующих функционирование ИАС; - опытом управления работой коллектива информационно-аналитических работников; - опытом управления работой специалистов по созданию и эксплуатации информационно-аналитических систем и средств защиты информации; - опытом представления информации в систематизированном виде, оформления научно-технического отчета или материала для выступления или публикации. - опытом организации работ по созданию и эксплуатации информационной безопасности защищаемого объекта на разных этапах жизненного цикла; - навыками разработки методических документов, регламентирующих функционирование ИАС; - опытом управления работой коллектива информационно-аналитических работников; - опытом управления работой специалистов по созданию и эксплуатации информационно-аналитических систем и средств защиты информации; - опытом представления информации в систематизированном виде, оформления научно-технического отчета или материала для выступления или публикации. - культурой стратегического мышления, навыками постановки целей и выбора способов их достижения;

				- навыками разработки и реализации стратегии организации.
ПК-4	Способен разрабатывать и применять нормативно-правовую, руководящую и методическую, а также организационно-распорядительную документацию, регламентирующую создание и функционирование информационно-аналитических систем в сфере профессиональной деятельности	ПК-4.1 Применяет нормативную правовую, организационно-распорядительную и методическую документацию, регламентирующую процесс создания и эксплуатации информационно-аналитических систем и обеспечение защиты информации. ПК-4.2 Разрабатывает проекты нормативной, методической и организационно-распорядительной документации, регламентирующей функционирование информационно-аналитических систем в соответствии с методами организационного обеспечения процесса разработки документов. ПК-4.3 Разрабатывает проекты нормативно-распорядительных документов (приказы, указания, инструкции) по	*ПОРОГОВЫЙ («удовлетворительно»)*	*Выпускник знает:* - содержание нормативных документов, регламентирующих порядок эксплуатации и создания информационно-аналитических систем, проведения аттестации объектов информатизации; - нормативную базу, регламентирующую деятельность по созданию информационно-аналитических систем; - нормативные правовые акты в области защиты информации; - руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; - основные методы организационного обеспечения процесса разработки документов, регламентирующих функционирование ИАС - нормативные правовые акты, стандарты и спецификации в области информационной безопасности - категорийный и понятийный аппарат в области оперативно-розыскной деятельности; - правовую и методическую основу оперативно-розыскной деятельности. - категорийный и понятийный аппарат в области конфиденциального делопроизводства; - структуру, сущность и особенности защищенного документооборота; - порядок осуществления доступа к документам ограниченного доступа, их подготовке, изданию, учету, движению и уничтожению. *Выпускник умеет:* - составлять техническое предложение на разработку информационно-аналитических систем; - разрабатывать программы аттестационных испытаний, протоколы; - применять нормативно-правовую, руководящую и методическую документацию; - разрабатывать проекты нормативно-распорядительных документов (приказы, указания) по вопросам создания ИАС; - разрабатывать проекты нормативных документов, регламентирующих функционирование ИАС; - разрабатывать проекты организационно-распорядительных документов, регламентирующих функционирование ИАС. - ориентироваться при разработке организаци-

		вопросам создания информационно-аналитических систем.		онных и нормативно-методических материалов в целях обеспечения информационной безопасности - осуществлять проверочные мероприятия в области информационной безопасности. - определять состав документов ограниченного доступа; - осуществлять подготовку документов ограниченного доступа, их учет, движение. *Выпускник владеет:* - навыками документированного обоснования требуемых характеристик защищенных информационно-аналитических систем; - навыками разработки документации на проектируемые защищенные информационно-аналитические системы и аттестованные объекты информатизации (разработка, оформление, согласование, утверждение в соответствии с требованиями нормативных документов); - навыками разработки нормативных документов, регламентирующих функционирование ИАС; - навыками разработки организационно-распорядительных документов, регламентирующих ИАС. - методиками, инструментарием использования компьютерной техники и информационных технологий при оформлении документации, связанной с международными и Российскими актами и стандартами информационной безопасности; - понятийным аппаратом документов, касающихся результатов ОРМ. - навыками организации процесса работы с документами ограниченного доступа – их подготовку, учет, движение, хранение, сдача в архив, уничтожение.
			БАЗОВЫЙ («хорошо»)	*Выпускник знает:* - содержание нормативных документов, регламентирующих порядок эксплуатации и создания информационно-аналитических систем, проведения аттестации объектов информатизации; - базовые требования, предъявляемые к документации на разрабатываемые и эксплуатируемые защищенные информационно-аналитические системы, аттестованные объекты информатизации; - нормативную правовую и методическую до-

				кументацию, регламентирующую деятельность по созданию и эксплуатации информационно-аналитических систем; - нормативные правовые акты в области защиты информации; - руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; - основные методы организационного обеспечения процесса разработки документов, регламентирующих функционирование ИАС – нормативные правовые акты, стандарты и спецификации в области информационной безопасности; – порядок разработки организационно-распорядительных документов в области обеспечения информационной безопасности. - категорийный и понятийный аппарат в области оперативно-розыскной деятельности; - правовую и методическую основу оперативно-розыскной деятельности; - сущность методов и способов осуществления оперативно-розыскных мероприятий в области информационной безопасности. - категорийный и понятийный аппарат в области конфиденциального делопроизводства; - структуру, сущность и особенности защищенного документооборота; - порядок осуществления доступа к документам ограниченного доступа, их подготовке, изданию, учету, движению, архивированию и уничтожению; - требования к помещениям, предназначенным для хранения и работы с документами ограниченного доступа. *Выпускник умеет:* - составлять техническое предложение на разработку информационно-аналитических систем; - разрабатывать программы и методики аттестационных испытаний, протоколы; - применять нормативно-правовую, руководящую и методическую документацию; - разрабатывать проекты нормативно-распорядительных документов (приказы, указания) по вопросам создания и эксплуатации ИАС; - разрабатывать проекты нормативных документов, регламентирующих функционирование ИАС; - разрабатывать проекты организационно-распорядительных документов, регламенти-

				рующих функционирование ИАС - ориентироваться при разработке организационных и нормативно-методических материалов в целях обеспечения информационной безопасности - применять методы ОРМ при проведении проверочных мероприятий; - осуществлять сбор необходимых документов. - определять состав документов ограниченного доступа; - осуществлять подготовку документов ограниченного доступа, их учет, движение, хранение, архивирование, уничтожение. *Выпускник владеет:* - навыками документированного обоснования требуемых характеристик защищенных информационно-аналитических систем; - навыками разработки документации на проектируемые защищенные информационно-аналитические системы и аттестованные объекты информатизации (разработка, оформление, согласование, утверждение в соответствии с требованиями нормативных документов); - навыками использования нормативной базы РФ, международных стандартов; - навыками разработки нормативных документов, регламентирующих функционирование ИАС; - навыками разработки организационно-распорядительных документов, регламентирующих ИАС; - опытом представления информации в систематизированном виде - методиками, инструментарием использования компьютерной техники и информационных технологий при оформлении документации, связанной с международными и Российскими актами и стандартами информационной безопасности; - методологией ОРД; - навыками документирования результатов проверочных мероприятий. - навыками организации процесса работы с документами ограниченного доступа – их подготовку, учет, движение, хранение, сдача в архив, уничтожение; - навыками организации процесса по обеспечению защиты документов ограниченного доступа.
			ПОВЫШ	*Выпускник знает:*

			ЕННЫЙ («отлично»)	- содержание нормативных документов, регламентирующих порядок эксплуатации и создания информационно-аналитических систем, проведения аттестации объектов информатизации; - требования, предъявляемые к документации на разрабатываемые и эксплуатируемые защищенные информационно-аналитические системы, аттестованные объекты информатизации; - нормативную правовую и методическую документацию, регламентирующую деятельность по созданию, эксплуатации и модернизации информационно-аналитических систем; - нормативные правовые акты в области защиты информации; - руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; - основные методы организационного обеспечения процесса разработки документов, регламентирующих функционирование ИАС – нормативные правовые акты, стандарты и спецификации в области информационной безопасности; порядок разработки организационно-распорядительных документов в области обеспечения информационной безопасности - категорийный и понятийный аппарат в области оперативно-розыскной деятельности; - правовую и методическую основу оперативно-розыскной деятельности; - распределение функций и обязанностей органов, осуществляющих оперативно-розыскную деятельность; - сущность методов и способов осуществления оперативно-розыскных мероприятий в области информационной безопасности. - категорийный и понятийный аппарат в области конфиденциального делопроизводства; - структуру, сущность и особенности защищенного документооборота; - порядок осуществления доступа к документам ограниченного доступа, их подготовке, изданию, учету, движению и уничтожению; - требования к помещениям, предназначенным для хранения и работы с документами ограниченного доступа. *Выпускник умеет:* - составлять техническое предложение на разработку информационно-аналитических си-

				стем; - разрабатывать программы и методики аттестационных испытаний, протоколы и заключения; - применять нормативно-правовую, руководящую и методическую документацию; - разрабатывать проекты нормативно-распорядительных документов (приказы, указания, инструкции) по вопросам создания и эксплуатации ИАС; - разрабатывать проекты нормативных документов, регламентирующих функционирование ИАС; - разрабатывать проекты организационно-распорядительных документов, регламентирующих функционирование ИАС - ориентироваться при разработке организационных и нормативно-методических материалов в целях обеспечения информационной безопасности - осуществлять проверочные мероприятия в области информационной безопасности; - осуществлять сбор и анализ полученной информации; - разрабатывать и планировать проверочные мероприятия. - определять состав документов ограниченного доступа; - осуществлять подготовку документов ограниченного доступа, их учет, движение, хранение, уничтожение; - обеспечивать защиту документов ограниченного доступа. *Выпускник владеет:* - навыками документированного обоснования требуемых характеристик защищенных информационно-аналитических систем; - навыками разработки документации на проектируемые защищенные информационно-аналитические системы и аттестованные объекты информатизации (разработка, оформление, согласование, утверждение в соответствии с требованиями нормативных документов); - навыками использования нормативной базы РФ, международных, зарубежных стандартов, лучших практик по проведению аттестации объектов информатизации; - навыками разработки нормативных документов, регламентирующих функционирование ИАС; - навыками разработки организационно-распорядительных документов, регламенти-

				рующих ИАС; - опытом представления информации в систематизированном виде, оформления научно-технического отчета или материала для выступления или публикации - методиками, инструментарием использования компьютерной техники и информационных технологий при составлении и оформлении документации, связанной с международными и Российскими актами и стандартами информационной безопасности - методами форензики; - навыками критического анализа полученных материалов; - навыками документирования результатов проведенных мероприятий. - навыками организации процесса работы с документами ограниченного доступа – их подготовку, учет, движение, хранение, сдача в архив, уничтожение; - навыками организации процесса по обеспечению защиты документов ограниченного доступа; - навыками применения правовых, нормативных и организационно-распорядительных документов, регламентирующих порядок работы с документами ограниченного доступа.

3.2 Показатели, критерии и шкалы оценивания компетенций

Каждому из уровней сформированности компетенций соответствует оценка «отлично» (5), «хорошо» (4) и «удовлетворительно» (3) в соответствии с установленной шкалой оценивания.

Таблица 2

Шкала оценивания сформированности компетенций

Уровни сформированности компетенций	Пороговый	Базовый	Повышенный
Шкала оценивания	Оценка «удовлетворительно» / «зачтено»	Оценка «хорошо» / «зачтено»	Оценка «отлично» / «зачтено»
Критерии оценивания	Компетенция сформирована. Демонстрируется недостаточный уровень самостоятельности практического навыка	Компетенция сформирована. Демонстрируется достаточный уровень самостоятельности устойчивого практического навыка	Компетенция сформирована. Демонстрируется высокий уровень самостоятельности, высокая адаптивность практического навыка

4 МЕСТО ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ В СТРУКТУРЕ ООП

Государственная итоговая аттестация входит в блок Б.3 «Государственная итоговая аттестация» «Государственная итоговая аттестация» ООП высшего образования – программы магистратуры федерального государственного образовательного стандарта высшего образования (далее – ФГОС ВО) по направлению подготовки 10.04.01 Информационная безопасность, профиль «Организация и управление информационной безопасностью».

Государственная итоговая аттестация проводится на 3-м курсе в 5-м семестре и включает в себя защиту выпускной квалификационной работы в форме магистерской диссертации.

Матрица поэтапного формирования компетенций, отражающая междисциплинарные связи, приведена в общей характеристике ООП по направлению подготовки.

5 МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ПОДГОТОВКЕ К ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

5.1 Требования к ВКР и методические рекомендации по подготовке ВКР

ВКР является важным этапом учебного процесса, направленным на подготовку высококвалифицированных специалистов. Выполнение ВКР является комплексной проверкой подготовки обучающегося к практической деятельности, а также важнейшей формой реализации приобретенных в процессе обучения навыков творческой, самостоятельной работы. Защита ВКР является одним из видов аттестационных испытаний, предусматриваемых государственной аттестацией.

Выпускная квалификационная работа (ВКР) в форме магистерской представляет собой комплексную, самостоятельную работу обучающегося, главная цель и содержание которой – всесторонний анализ, научные исследования или разработки по одному из вопросов теоретического или практического характера, соответствующих профилю направления подготовки.

Перечень ВКР, утверждаемых выпускающей кафедрой и предлагаемых обучающимся, доводится до сведения обучающихся не позднее чем за 6 месяцев до начала ГИА посредством ознакомления обучающихся с перечнем примерных тем выпускных квалификационных работ под роспись в листе ознакомления.

Примерные темы ВКР по ООП высшего образования федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.04.01 Информационная безопасность, профиль «Организация и управление информационной безопасностью»:

1. Разработка имитационной компьютерной модели для виртуальных исследований информационных систем.
2. Оценка эффективности средств защиты информации в государственных информационных системах.
3. Разработка методики по проверке соответствия жизненного цикла программного обеспечения стандарту Secure SDLC
4. Разработка защищенного Web-интерфейса для управления техническими системами.
5. Оценка соответствия средств защиты информации на значимых объектах критической информационной инфраструктуры РФ.
6. Исследование методов обеспечения целостности информации.
7. Разработка имитационной компьютерной модели для виртуальных исследований информационных систем.
8. Защита информации в распределенной информационной системе предприятия ОПК.
9. Разработка подсистемы защиты информационного проекта предприятия от несанкционированного доступа.
10. Исследование надежности и безопасности функционирования фотоприемников систем контроля изображения.
11. Создание инфраструктуры обработки и защиты информации с использованием технологий виртуализации.
12. Разработка методики цифровой обработки сигналов в системах информационной безопасности.

13. Разработка методики тестирования на проникновение элементов инфраструктуры обработки информации.

14. Разработка конструкции экранов для снижения уровня электромагнитного излучения компьютера.

15. Разработка программного обеспечения для компьютерного моделирования технических систем информационного типа.

16. Планирование и разработка комплексной системы безопасности предприятия оборонно-промышленного комплекса.

17. Разработка информационной системы для ведение реестра значимых объектов критическое информационной инфраструктуры.

18. Организация и обеспечение информационной безопасности образовательного Интернета вещей.

19. Использование программного средства защиты информации MaxPatrol в учебном процессе образовательного учреждения.

20. Создание виртуальной лаборатории компьютерной безопасности.

21. Исследование эффективности методов защиты оптических каналов передачи информации в Интернете-вещей.

22. Математическая модель политики информационной безопасности объекта информатизации, обрабатывающего персональные данные.

23. Комплексная система защиты информации на примере предприятия Х.

24. Совершенствование управления информационной безопасностью в организации.

25. Совершенствование информационной безопасности в организации.

26. Разработка персонального межсетевого экрана с изолированным ядром.

27. Проектирование защищенной сети передачи данных предприятия Х.

28. Разработка защищённого сайта, содержащего сведения коммерческой тайны и персональные данные пользователей системы CRM.

29. Разработка методики обеспечения информационной безопасности АБИС "ИРБИС-64+".

30. Комплексная система защиты электронного документооборота.

31. Исследования методов защиты информации в сетях передачи данных.

32. Исследование уязвимостей алгоритмов защиты информации.

33. Совершенствование организационного обеспечения защиты информации при предоставлении сведений Единого государственного реестра недвижимости.

34. Аудит значимых объектов КИИ с использованием подходов ЦБ РФ.

35. Анализ и оценка безопасности защищённой локальной сети коммерческой организации АО «РиМ».

36. Эффективность затрат на информационную безопасность в организации.

37. Анализ возможной интеграции SAP инфраструктуры и центров ГосСОПКА

По письменному заявлению обучающегося кафедра может предоставить обучающемуся (обучающимся) возможность подготовки и защиты ВКР по теме, предложенной обучающимся (обучающимися), в случае обоснованности целесообразности ее разработки для практического применения в соответствующей области профессиональной деятельности или на конкретном объекте профессиональной деятельности. Для подготовки ВКР за обучающимся (несколькими обучающимися, выполняющими ВКР совместно) приказом ректора СГУГиТ закрепляется руководитель ВКР из числа работников СГУГиТ и при необходимости консультант (консультанты).

Целью выполнения выпускной квалификационной работы является не только закрепление полученных в период обучения знаний, но и расширение, дополнение полученных в вузе знаний по общетеоретическим и специальным дисциплинам, а также развитие необходимых навыков самостоятельной научной работы.

В ходе подготовки ВКР решаются следующие задачи:

– самостоятельное исследование актуальных вопросов профессиональной деятельности;

– систематизация, закрепление и расширение теоретических знаний по специальным дисциплинам;

– углубление навыков ведения обучающимся самостоятельной исследовательской работы, работы с различной справочной и специальной литературой, финансовой отчетностью организаций;

– овладение методологией исследования при решении разрабатываемых в ВКР проблем;

– изучение и использование современных информационных технологий и технологий защиты информации.

При выполнении ВКР обучающийся демонстрирует свою способность, опираясь на полученные знания, умения и сформированные общекультурные, общепрофессиональные и профессиональные компетенции, самостоятельно решать на современном уровне задачи своей профессиональной деятельности, профессионально излагать специальную информацию, научно аргументировать и защищать свою точку зрения.

ВКР должна содержать: обоснование выбора темы исследования, анализ разработанности данной проблематики в отечественной и зарубежной научной литературе, постановку цели и задач исследования. В ВКР дается последовательное и обстоятельное изложение полученных результатов, и на их основе формулируются четкие выводы. В заключении ВКР должен быть представлен список использованной литературы. При необходимости в ВКР могут быть включены дополнительные материалы (графики, таблицы и т.д.), которые оформляются в виде приложений.

Выпускная квалификационная работа должна соответствовать требованиям СТО СГУГиТ 8-06-2021. Стандарт организации. Система менеджмента качества. Государственная итоговая аттестация выпускников СГУГиТ. Структура и правила оформления.

В соответствии с Положением о порядке проведения проверки письменных работ на наличие заимствований в ФГБОУ ВО «Сибирский государственный университет геосистем и технологий» оформленная ВКР должна пройти оценку на наличие неправомочных заимствований. При не устранении неправомочных заимствований после (или неспособности обучающегося в силу различных причин устранить их в установленные положением сроки), работа не допускается к защите.

ВКР допускается к защите только после ее предварительного утверждения заведующим выпускающей кафедры при наличии положительного отзыва руководителя и рецензии.

Защита ВКР проводится на заседании Государственной экзаменационной комиссии (ГЭК). Результаты защиты ВКР являются основанием для принятия Государственной экзаменационной комиссией решения о присвоении соответствующей квалификации (степени) и выдаче диплома государственного образца.

В процессе подготовки ВКР научный руководитель ВКР содействует обучающемуся в выборе темы ВКР и разработке плана ее выполнения; оказывает помощь в выборе методики проведения исследования и организации процесса написания ВКР; проводит консультации по подбору нормативных документов, литературы, статистического и фактического материала; осуществляет систематический контроль за полнотой и качеством подготавливаемых разделов ВКР в соответствии с разработанным планом и своевременным представлением работы на кафедру; составляет письменный отзыв о работе; проводит подготовку и предварительную защиту ВКР с целью выявления готовности обучающегося к защите; принимает участие в защите ВКР и несет ответственность за качество представленной к защите ВКР.

При подготовке к защите ВКР, обучающемуся необходимо составить тезисы или конспект своего выступления, согласовать его с руководителем.

5.2 Методические рекомендации по процедуре защиты ВКР

Выпускающая кафедра обеспечивает ознакомление обучающегося с отзывом и рецензией не позднее чем за 5 календарных дней до дня защиты ВКР. ВКР, отзыв и рецензия передаются в государственную экзаменационную комиссию не позднее чем за 2 календарных дня до даты защиты ВКР.

Для защиты рассматриваемых в работе положений, обоснования выводов при необходимости можно подготовить наглядные материалы: таблицы, графики, диаграммы и обращаться к ним в ходе защиты.

В СГУГиТ установлена единая процедура защиты ВКР. Аудитория для проведения защиты должна быть оснащена мультимедийным оборудованием для демонстрации электронной презентации.

К началу защиты ВКР в аудитории должны быть подготовлены:

– приказ о составе ГЭК;
– сведения о выпускниках, допущенных к защите;
– ведомости;
– протоколы ГЭК.

Согласно этой процедуре защита ВКР проводится на открытом заседании ГЭК, состав которой утверждается ректором СГУГиТ. Защита осуществляется каждым обучающимся индивидуально на открытых заседаниях ГЭК с участием не менее двух третей ее состава, как правило, при непосредственном участии руководителя работы.

Процедура защиты следующая. Председатель ГЭК или ее член знакомит присутствующих с темой работы и предоставляет слово для выступления обучающемуся. Обучающийся излагает основные положения своей работы, акцентируя внимание присутствующих на выводах и предложениях. В выступлении следует обосновать актуальность темы, новизну рассматриваемых проблем и выводов, степень разработанности темы, кратко изложить основное содержание, выводы и предложения с убедительной аргументацией. Обучающийся должен излагать основное содержание своей работы свободно, не читая письменный текст. При этом необходимо учитывать, что на выступление обучающегося отводится не более 15 минут. После выступления обучающегося комиссия, а также все присутствующие задают вопросы по теме работы, представленной на защиту.

На вопросы обучающийся отвечает, как правило, непосредственно после доклада, но возможна с согласия ГЭК дополнительная подготовка. При необходимости обучающийся может пользоваться пояснительной запиской ВКР. После ответа на вопросы предоставляется слово научному руководителю.

Решение ГЭК об оценке ВКР принимается на закрытом заседании с учетом отзыва научного руководителя и рецензии, содержания вступительного слова, кругозора выпускника, его умения выступить публично, защитить свои интересы, глубины ответов на вопросы, отзывов заказчика (по заказным темам).

Защита ВКР имеет целью оценить готовность выпускника к профессиональной деятельности.

Критериями оценки ВКР на ее защите в ГЭК должны быть:

– соответствие содержания и оформления ВКР установленным требованиям;
– степень выполнения выпускником полученных от кафедры заданий на разработку конкретных вопросов темы ВКР;
– глубина разработки рассматриваемых в работе проблем, насыщенность практическим материалом;
– значимость сделанных в работе выводов и предложений и степень их обоснованности;
– зрелость выступления выпускника на защите ВКР: логика изложения своих рекомендаций, полнота ответов на заданные вопросы, качество ответов на замечания присутствующих на защите.

Результат защиты определяется оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» и объявляется в тот же день после оформления в установленном порядке протоколов заседаний ГЭК по защите ВКР.

Примерные вопросы, задаваемые при публичной защите ВКР:

1 Сформулируйте актуальность ВКР.
2 Сформулируйте цель ВКР.
3 Сформулируйте задачи проведенного исследования.
4 Определите степень разработанности проблемы.
5 Сформулируйте выводы по полученным результатам исследования.
6 Перечислите рекомендации по практической реализации полученных результатов.

Организация проведения защиты ВКР для инвалидов и лиц с ограниченными возможностями здоровья проводится в соответствии с Приказом Минобрнауки России от 29.06.2015 N 636 "Об утверждении Порядка проведения государственной итоговой аттестации по образовательным программам высшего образования - программам бакалавриата, программам специалитета и программам магистратуры".

5.3 Порядок подачи и рассмотрения апелляций

Апелляция подается лично обучающимся в апелляционную комиссию не позднее следующего рабочего дня после объявления результатов государственного аттестационного испытания. Для рассмотрения апелляции секретарь государственной экзаменационной комиссии направляет в апелляционную комиссию протокол заседания государственной экзаменационной комиссии, заключение председателя государственной экзаменационной комиссии о соблюдении процедурных вопросов при проведении государственного аттестационного испытания, а также письменные ответы обучающегося (при их наличии) (для рассмотрения апелляции по проведению государственного экзамена) либо выпускную квалификационную работу, отзыв и рецензию (рецензии) (для рассмотрения апелляции по проведению защиты выпускной квалификационной работы).

Апелляция не позднее 2 рабочих дней со дня ее подачи рассматривается на заседании апелляционной комиссии, на которое приглашаются председатель государственной экзаменационной комиссии и обучающийся, подавший апелляцию. Заседание апелляционной комиссии может проводиться в отсутствие обучающегося, подавшего апелляцию, в случае его неявки на заседание апелляционной комиссии.

Решение апелляционной комиссии доводится до сведения обучающегося, подавшего апелляцию, в течение 3 рабочих дней со дня заседания апелляционной комиссии. Факт ознакомления обучающегося, подавшего апелляцию, с решением апелляционной комиссии удостоверяется подписью обучающегося.

При рассмотрении апелляции о нарушении процедуры проведения государственного аттестационного испытания апелляционная комиссия принимает одно из следующих решений: об отклонении апелляции, если изложенные в ней сведения о нарушениях процедуры проведения государственного аттестационного испытания обучающегося не подтвердились и (или) не повлияли на результат государственного аттестационного испытания; об удовлетворении апелляции, если изложенные в ней сведения о допущенных нарушениях процедуры проведения государственного аттестационного испытания обучающегося подтвердились и повлияли на результат государственного аттестационного испытания.

При рассмотрении апелляции о несогласии с результатами государственного экзамена апелляционная комиссия выносит одно из следующих решений: об отклонении апелляции и сохранении результата государственного экзамена; об удовлетворении апелляции и выставлении иного результата государственного экзамена.

Решение апелляционной комиссии не позднее следующего рабочего дня передается в государственную экзаменационную комиссию. Решение апелляционной комиссии является основанием для аннулирования ранее выставленного результата государственного экзамена и выставления нового.

Решение апелляционной комиссии является окончательным и пересмотру не подлежит.

Повторное проведение государственного аттестационного испытания обучающегося, подавшего апелляцию, осуществляется в присутствии председателя или одного из членов апелляционной комиссии не позднее даты завершения обучения в организации в соответствии со стандартом.

Апелляция на повторное проведение государственного аттестационного испытания не принимается.

6 ОЦЕНОЧНЫЕ СРЕДСТВА ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

6.1 Паспорт фонда оценочных средств по ГИА

Уровень сформированности компетенции выпускника определяется комплексно на основе следующих компонентов ГИА: отзыва руководителя ВКР, рецензии, качества выполненной работы, защиты ВКР.

Степень сформированности компетенций выпускника и уровень их освоения определяется в период ГИА, в различных ее компонентах. Оценочные материалы для ГИА выпускников включают показатели и критерии оценки результата выполнения и защиты ВКР.

Компетенции и компоненты их оценки в период ГИА

Таблица 5

Код компетенции	Содержание компетенции	Код и наименование индикатора достижения	Компонент ГИА, в которой проводится оценка уровня сформированности компетенций
УК-1	Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.1. Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними. УК-1.2. Осуществляет поиск вариантов решения поставленной проблемной ситуации на основе доступных источников информации. УК-1.3. Разрабатывает стратегию достижения поставленной цели как последовательность шагов, предвидя результат каждого из них и оценивая их влияние на внешнее окружение планируемой деятельности и на взаимоотношения участников этой деятельности.	Отзыв руководителя, рецензия, текст ВКР
УК-2	Способен управлять проектом на всех этапах его жизненного цикла	УК-2.1. Формулирует в рамках обозначенной проблемы, цель, задачи, актуальность, значимость (научную, практическую, методическую и иную в зависимости от типа проекта), ожидаемые результаты и возможные сферы их применения УК-2.2. Способен представлять результат деятельности и планировать последовательность шагов для достижения данного результата. Формирует план-график реализации проекта в целом и план контроля его выполнения УК-2.3. Организует и координирует работу участников проекта, способствует конструктивному преодолению возникающих разногласий и конфликтов, обеспечивает работу команды необходимыми ресурсами УК-2.4. Представляет публично результаты проекта (или отдельных его этапов) в форме отчетов, статей, выступлений на научно-практических конференциях,	Отзыв руководителя, рецензия, текст ВКР

		семинарах и т.п.	
УК-3	Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	УК-3.1. Организует и координирует работу участников проекта, способствует конструктивному преодолению возникающих разногласий и конфликтов УК-3.2. Учитывает в своей социальной и профессиональной деятельности интересы, особенности поведения и мнения (включая критические) людей, с которыми работает/взаимодействует, в том числе посредством корректировки своих действий УК-3.3. Предвидит результаты (последствия) как личных, так и коллективных действий УК-3.4. Планирует командную работу, распределяет поручения и делегирует полномочия членам команды. Организует обсуждение разных идей и мнений	Отзыв руководителя, рецензия, текст ВКР
УК-4	Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	УК-4.1. Демонстрирует интегративные умения, необходимые для написания, письменного перевода и редактирования различных академических текстов (рефератов, эссе, обзоров, статей и т.д.) УК-4.2. Представляет результаты академической и профессиональной деятельности на различных научных мероприятиях, включая международные УК-4.3. Демонстрирует интегративные умения, необходимые для эффективного участия в академических и профессиональных дискуссиях	Отзыв руководителя, рецензия, текст ВКР
УК-5	Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	УК-5.1. Адекватно объясняет особенности поведения и мотивации людей различного социального и культурного происхождения в процессе взаимодействия с ними, опираясь на знания причин появления социальных обычаев и различий в поведении людей УК-5.2. Владеет навыками создания недискриминационной среды взаимодействия при выполнении профессиональных задач	Отзыв руководителя, рецензия, текст ВКР
УК-6	Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки	УК-6.1. Определяет приоритеты своей деятельности, выстраивает и реализовывает траекторию саморазвития на основе мировоззренческих принципов УК-6.2. Использует личностный потенциал в социальной среде для достижения поставленный целей УК-6.3. Демонстрирует социальную ответственность за принимаемые решения, учитывает правовые и культурные аспекты, обеспечивает устойчивое развитие при ведении профессиональной и иной деятельности УК-6.4.	Отзыв руководителя, рецензия, текст ВКР

		Оценивает свою деятельность, соотносит цели, способы и средства выполнения деятельности с её результатами	
ОПК-1	Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	ОПК-1.1. Анализирует систему обеспечения информационной безопасности и формулирует требования по ее улучшению. ОПК-1.2. Разрабатывает проект технического задания на создание системы обеспечения информационной безопасности.	Отзыв руководителя, рецензия, текст ВКР
ОПК-2	Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности	ОПК-2.1. Разрабатывает технический проект системы (подсистемы, компоненты системы) обеспечения информационной безопасности в соответствии с техническим заданием, нормативно-правовой, организационно-распорядительной и методической документацией.	Отзыв руководителя, рецензия, текст ВКР
ОПК-3	Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности	ОПК-3.1. Разрабатывает проекты организационно-распорядительной документации, регламентирующих процесс обеспечения информационной безопасности	Отзыв руководителя, рецензия, текст ВКР
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-4.1. Осуществляет поиск научно-технической информации для решения поставленной задачи, обработку и анализ собранных данных. ОПК-4.2. Осуществляет планирование эксперимента, разрабатывает программу проведения исследований.	Отзыв руководителя, рецензия, текст ВКР
ОПК-5	Способен про-	ОПК-5.1.	Отзыв руко-

	водить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи	Проводит исследования в соответствии с разработанным планом и программой. ОПК-5.2. Обрабатывает полученные результаты с применением методом математической статистики. ОПК-5.3. Осуществляет подготовку научно-технических отчетов, аналитических обзоров, научных докладов и статей.	водителя, рецензия, текст ВКР
ПК-1	Способен выявлять основные тенденции развития в области информационной безопасности, прогнозировать потенциальные угрозы и риски в работе информационно-аналитических систем, обеспечивать защиту информации	ПК-1.1 Осуществляет функционирование процесса обеспечения безопасности информационно-аналитических систем. ПК-1.2 Выявляет, классифицирует и оценивает уязвимости информационно-аналитических систем, угрозы и риски безопасности. ПК-1.3 Определяет требования к техническим и программным средствам защиты информации в информационно-аналитических системах, проводит обоснование характеристик и функциональных возможностей средств обеспечения информационной безопасности информационно-аналитических систем. ПК-1.4 Осуществляет подбор средств и технологий защиты в информационно-аналитических системах и оценку их эффективности	Отзыв руководителя, рецензия, текст ВКР
ПК-2	Способен осуществлять работу по проектированию, разработке информационно-аналитических систем	ПК-2.1 Разрабатывает проектно-технические решения, осуществляет формирование технического состава системы, определяет номенклатуру применяемого оборудования и материалов, места установки элементов системы. ПК-2.2 Разрабатывает документацию на проектируемые и модернизируемые информационно-аналитические системы	Отзыв руководителя, рецензия, текст ВКР
ПК-3	Способен проводить исследования по разработке и усовершенствованию информационно-аналитических систем, обра-	ПК-3.1 Проводит критический анализ фундаментальных и прикладных проблем информационно-аналитической системы в современных условиях. ПК-3.2 Осуществляет поиск и анализ научно-технической информации, выбор технологий, методов и способов решения профессиональных задач, разрабатывает планы и программы проведения научных исследо-	Отзыв руководителя, рецензия, текст ВКР

	батывать и анализировать полученные результаты	ваний и технических разработок. ПК-3.3 Проводит экспериментальные исследования по оценке защищенности информационно-аналитических систем с применением фундаментальных закономерностей, физических и математических методов, технических и программных средств; обрабатывает полученные результаты, оформляет научно-технические отчеты, готовит обзоры, научные статьи и доклады. ПК-3.4 Осуществляет внедрение, адаптацию, настройку и интеграцию проектных решений по созданию защищенных информационно-аналитических систем.	
ПК-4	Способен организовать работу по созданию, эксплуатации и модернизации информационно-аналитических систем	ПК-4.1 Организует выполнение работ и управляет работой коллектива по эксплуатации информационно-аналитических и экспертных систем. ПК-4.2 Организует выполнение работ и управляет работой коллектива по созданию и модернизации информационно-аналитических и экспертных систем. ПК-4.3 Принимает управленческие решения и оценивает их эффективность для обеспечения безопасности информационно-аналитических систем в соответствии с требованиями нормативной правовой и организационно-методической документации.	Отзыв руководителя, рецензия, текст ВКР
ПК-5	Способен разрабатывать и применять нормативно-правовую, руководящую и методическую, а также организационно-распорядительную документацию, регламентирующую создание и функционирование информационно-аналитических систем в сфере профессиональной деятельности	ПК-5.1 Применяет нормативную правовую, организационно-распорядительную и методическую документацию, регламентирующую процесс создания и функционирования информационно-аналитических систем. ПК-5.2 Разрабатывает нормативную, методическую и организационно-распорядительную документацию, необходимую для создания и функционирования информационно-аналитических систем. ПК-5.3 Разрабатывает программы и методики испытаний информационно-аналитических систем и средств обеспечения информационной безопасности	Отзыв руководителя, рецензия, текст ВКР

6.2 Критерии оценки ВКР научным руководителем и рецензентом

Оформленная ВКР передается на отзыв руководителю, который оформляется в соответствии с СТО СГУГиТ 8-06-2021. Стандарт организации. Система менеджмента качества. Государственная итоговая аттестация выпускников СГУГиТ. Структура и правила оформления.

Критерии оценки уровня освоения компетенций на основе отзыва руководителя и рецензии рецензента

Код компетенции	Содержание компетенции	Уровень сформированности компетенций повышенный (оценка «отлично»), базовый (оценка «хорошо»), пороговый (оценка «удовлетворительно»)
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	
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	
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.	
ПК-1	Способен выявлять основные тенденции развития	

	в области информационной безопасности, прогнозировать потенциальные угрозы и риски в работе информационно-аналитических систем, обеспечивать защиту информации	
ПК-2	Способен осуществлять работу по проектированию, разработке информационно-аналитических систем	
ПК-3	Способен проводить исследования по разработке и усовершенствованию информационно-аналитических систем, обрабатывать и анализировать полученные результаты	
ПК-4	Способен организовать работу по созданию, эксплуатации и модернизации информационно-аналитических систем	
ПК-5	Способен разрабатывать и применять нормативно-правовую, руководящую и методическую, а также организационно-распорядительную документацию, регламентирующую создание и функционирование информационно-аналитических систем в сфере профессиональной деятельности	
Итоговая оценка	*Примечание: оценка «отлично» выставляется, если средний балл по всем критериям получен не ниже 4,6; оценка «хорошо» выставляется, если средний балл по всем критериям получен не ниже 3,6; оценка «удовлетворительно» выставляется, если по всем критериям оценки положительные; оценка «неудовлетворительно», если получено по критериям одна и более неудовлетворительных оценок.*	

6.3 Критерии оценки защиты ВКР членами ГЭК

Заседания комиссий правомочны, если в них участвуют не менее двух третей от числа лиц, входящих в состав комиссий. Заседания комиссий проводятся председателями комиссий. Решения комиссий принимаются простым большинством голосов от числа лиц, входящих в состав комиссий и участвующих в заседании. При равном числе голосов председатель комиссии обладает правом решающего голоса.

Решения, принятые комиссиями, оформляются протоколами.

В протоколе заседания государственной экзаменационной комиссии по приему государственного аттестационного испытания отражаются перечень заданных обучающемуся вопросов и характеристика ответов на них, мнения председателя и членов государственной экзаменационной комиссии о выявленном в ходе государственного аттестационного испытания уровне подготовленности обучающегося к решению профессиональных задач, а также о выявленных недостатках в теоретической и практической подготовке обучающегося.

Протоколы заседаний комиссий подписываются председателем. Протокол заседания государственной экзаменационной комиссии также подписывается секретарем экзаменационной комиссии.

Критериями оценки ВКР на ее защите в ГЭК должны быть:

- соответствие содержания и оформления ВКР с СТО СГУГиТ 8-06-2021 Стандарт организации. Система менеджмента качества. Государственная итоговая аттестация выпускников СГУГиТ. Структура и правила оформления;

- степень выполнения выпускником полученных от руководителя ВКР заданий на разработку конкретных вопросов темы ВКР;

- глубина разработки рассматриваемых в работе проблем, насыщенность практическим материалом;

значимость сделанных в работе выводов и предложений и степень их обоснованности;

- зрелость выступления выпускника на защите ВКР: логика изложения своих рекомендаций, полнота ответов на заданные вопросы, качество ответов на замечания присутствующих на защите.

Результат защиты определяется оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» и объявляется в тот же день после оформления в установленном порядке протоколов заседаний ГЭК по защите ВКР.

При выставлении оценки комиссия руководствуется примерными критериями оценки ВКР:

– «отлично» – выставляется за квалификационную работу, которая представляет собой самостоятельное и завершенное исследование, включает теоретический раздел, содержащий глубокий анализ научной проблемы и современного состояния ее изучения. Исследование реализовано на основании достаточной источниковой базы, с применением актуальных методологических подходов. Работа имеет положительный отзыв научного руководителя. При ее защите выпускник показывает глубокие знания вопросов темы исследования, свободно оперирует данными исследования, вносит обоснованные предложения, эффективно использует новые информационные технологии при презентации своего доклада, убедительно иллюстрируя доклад диаграммами, схемами, таблицами, графиками, уверенно отвечает на поставленные вопросы.

– «хорошо» – выставляется за квалификационную работу, которая носит исследовательский характер, имеет грамотно изложенный теоретический раздел, в котором представлены достаточно подробный анализ и критический разбор концептуальных подходов и практической деятельности, последовательное изложение материала с соответствующими выводами, но с недостаточно обоснованными предложениями. Работа имеет положительный отзыв научного руководителя. При ее защите выпускник показывает знание вопросов темы исследования, оперирует данными исследования, вносит предложения по теме исследования, во время доклада использует наглядный материал (таблицы, графики, схемы и пр.), без особых затруднений отвечает на поставленные вопросы;

– «удовлетворительно» – выставляется за квалификационную работу, которая содержит теоретическую главу, элементы исследования, базируется на практическом материале, но отсутствует глубокий анализ научной проблемы; в работе просматривается непоследовательность изложения материала; представленные предложения недостаточно обоснованы. В отзыве руководителя имеются замечания по содержанию работы. Во время защиты выпускник проявляет неуверенность, показывает слабое знание вопросов темы, не всегда дает обоснованные и исчерпывающие ответы на заданные вопросы, допускает существенные ошибки;

– «неудовлетворительно» – выставляется за квалификационную работу, которая не носит последовательного характера, не отвечает требованиям, изложенным в методических указаниях выпускающих кафедр. В работе нет выводов. В отзыве научного руководителя имеются существенные замечания. При защите работы выпускник затрудняется в ответах на поставленные вопросы, допускает существенные ошибки. К защите не подготовлены презентационные материалы и раздаточный материал.

Критерии оценки уровня освоения компетенций на основе выполненной ВКР, ее защиты, оформления и презентации

Оцениваемые компетенции	Показатели оценки ВКР	оценка «отлично»	оценка «хорошо»	оценка «удовлетворительно»
1. Показатели оценки по формальным критериям (пример)				
УК-1, УК-4	Использование литературы (достаточное количество актуальных источников, достаточность цитирования, использование нормативных документов, научной и справочной литературы)	повышенный	базовый	пороговый
УК-4, ОПК-2	Соответствие ВКР нормативным локальным актам «Государственная	повышенный	базовый	пороговый

	итоговая аттестация выпускников СГУГиТ. Структура и правила оформления», «Положение о порядке проведения проверки письменных работ на наличие заимствований»			
Средний балл				
2. Показатели оценки по содержанию (пример)				
УК-2	Введение содержит следующие обязательные элементы: актуальность темы и практическая значимость работы; цель ВКР, соответствующая заявленной теме; круг взаимосвязанных задач, определенных поставленной целью	повы-шенный	базо-вый	пороговый
УК-6, ПК-1, ПК-3	Содержательность и глубина теоретической, научно-исследовательской и практической проработки проблемы	повы-шенный	базо-вый	пороговый
ОПК-2, ОПК-3, ПК-2, ПК-4	Содержательность производственно-технологической характеристики объекта исследования и глубина проведённого анализа проблемы. Качество анализа проблемы, планирование и осуществление деятельности в области	повы-шенный	базо-вый	пороговый
ОПК-2, ОПК-3, ПК-5	Содержательность рекомендаций автора по совершенствованию технологических процессов, организационно-управленческой и проектно-изыскательской деятельности или устранению проблем в деятельности объекта исследования, выявленных по результатам проведенного анализа	повы-шенный	базо-вый	пороговый
ОПК-1, ОПК-2	Оригинальность и практическая значимость предложений и рекомендаций	повы-шенный	базо-вый	пороговый
Средний балл				
3. Показатели оценки защиты ВКР				
УК-3, УК-4, ОПК-2	Качество доклада (структурированность, полнота раскрытия решенных задач для достижения поставленной цели, аргументированность выводов, визуализации полученных результатов). Навыки публичной дискуссии, защиты собственных научных идей, предложений и рекомендаций	повы-шенный	базо-вый	пороговый
ОПК-2	Качество и использование презентационного материала (информативность, соответствие содержанию доклада, наглядность,	повы-шенный	базо-вый	пороговый

	достаточность)			
УК-4, УК-5	Ответы на вопросы комиссии (полнота, глубина, оригинальность мышления. Общий уровень культуры общения с аудиторией	повы-шенный	базо-вый	пороговый
Средний балл				
Итоговая оценка члена ГЭК	Примечание: оценка «отлично» выставляется, если средний балл по всем критериям получен не ниже 4,6; оценка «хорошо» выставляется, если средний балл по всем критериям получен не ниже 3,6; оценка «удовлетворительно» выставляется, если по всем критериям оценки положительные; оценка «неудовлетворительно», если получено по критериям одна и более неудовлетворительных оценок.			

Итоговая оценка за выполнение и защиту ВКР в ходе проведения ГИА выставляется обучающемуся с учетом всех полученных оценок по вышеуказанным критериям и показателям; отзыва руководителя ВКР; оценок членов ГЭК. Общая оценка ГЭК определяется как средняя арифметическая величина из всех оценок.

7 ПЕРЕЧЕНЬ РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ ДЛЯ ПОДГОТОВКИ К ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

7.1 Основная литература

№ п/п	Библиографическое описание	Количество экземпляров в библиотеке СГУГиТ
1.	Абденов, А. Ж. Анализ, описание и оценка функциональных узлов SIEM-системы : учебное пособие / А. Ж. Абденов, В. А. Трушин, К. Сулайман. — Новосибирск : НГТУ, 2018. — 122 с. — ISBN 978-5-7782-3603-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/118277 (дата обращения: 19.07.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
2.	Аникин, В. М. Диссертациеведение : пролегомены : монография / В. М. Аникин. — Саратов : СГУ, 2019. — 108 с. — ISBN 978-5-292-04577-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/148879 (дата обращения: 19.07.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
3.	Антонов, А. В. Системный анализ : учебник / А.В. Антонов. — 4-е изд., перераб. и доп. — Москва : ИНФРА-М, 2020. — 366 с. + Доп. материалы [Электронный ресурс]. — (Высшее образование). - ISBN 978-5-16-011865-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1062325 (дата обращения: 19.07.2021). – Режим доступа: по подписке.	Электронный ресурс
4.	Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 336 с. — (Высшее образование). — DOI: https://doi.org/10.29039/1761-6. - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1189326 (дата обращения: 15.09.2021). – Режим доступа: по подписке.	Электронный ресурс
5.	Безопасность разработки в Agile-проектах / Л. Белл, М. Брантон-Сполл, Р. Смит, Д. Бэрд ; перевод с английского А. А. Слинкин. — Москва : ДМК Пресс, 2018. — 448 с. — ISBN 978-5-97060-648-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL:	Электронный ресурс

	https://e.lanbook.com/book/123703 (дата обращения: 19.07.2021). — Режим доступа: для авториз. пользователей.	
6.	Васильева, Т. В. Введение в магистерскую программу : учебное пособие / Т. В. Васильева. — Томск : ТПУ, 2017. — 91 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/106754 (дата обращения: 10.07.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
7.	Величко, В. В. Модели и методы повышения живучести современных систем связи : монография / В. В. Величко, Г. В. Попков, В. К. Попков. — Москва : Горячая линия-Телеком, 2017. — 270 с. — ISBN 978-5-9912-0408-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111035 (дата обращения: 10.07.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
8.	Ворона, В. А. Концептуальные основы создания и применения системы защиты объектов : справочное пособие / В. А. Ворона, В. А. Тихонов. — Москва : Горячая линия-Телеком, 2017. — 196 с. — ISBN 978-5-9912-0240-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111040 (дата обращения: 19.07.2021— Режим доступа: для авториз. пользователей.	Электронный ресурс
9.	Вотинов, М. В. Хранение и защита компьютерной информации : учебное пособие / М. В. Вотинов. — Мурманск : МГТУ, 2017. — 82 с. — ISBN 978-5-86185-947-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/142646 (дата обращения: 07.07.2021). — Режим доступа: для авториз. пользователей.	
10.	Гвоздева, Т. В. Проектирование информационных систем. Стандартизация : учебное пособие для вузов / Т. В. Гвоздева, Б. А. Баллод. — 2-е изд., стер. — Санкт-Петербург : Лань, 2021. — 252 с. — ISBN 978-5-8114-7963-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/169810 (дата обращения: 19.07.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
11.	Губин, А. Н. Проектная оценка надежности информационных систем : учебное пособие / А. Н. Губин. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2019. — 77 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/180062 (дата обращения: 06.07.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
12.	Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками : учебное пособие / П. Н. Девянин. — 2-е изд., испр. и доп. — Москва : Горячая линия-Телеком, 2017. — 338 с. — ISBN 978-5-9912-0328-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111049 (дата обращения: 07.07.2021). — Режим доступа: для авториз. пользователей.	
13.	Елинский, В. И. Проблемы формирования языка оперативно-розыскной деятельности : монография / В. И. Елинский, Р. М. Жиров. — Нальчик : КБГУ, 2020. — 108 с. — ISBN 978-5-7558-0632-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/170826 (дата обращения: 06.07.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
14.	Жук, А. П. Защита информации [Электронный ресурс] : учеб. пособие / А. П. Жук, Е. П. Жук, О. М. Лепешкин, А. И. Тимошкин. – 2-е изд. – М. : ИЦ РИОР: НИЦ ИНФРА-М, 2019. – 400 с. – Режим доступа: http://znanium.com/catalog/product/1018901 – Загл. с экрана	Электронный ресурс
15.	Зайцев, А. П. Технические средства и методы защиты информации : учеб-	Электронный

	ник / А. П. Зайцев, Р. В. Мещеряков, А. А. Шелупанов. — 7-е изд., испр. — Москва : Горячая линия-Телеком, 2018. — 442 с. — ISBN 978-5-9912-0233-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111057 (дата обращения: 06.07.2021). — Режим доступа: для авториз. пользователей.	ресурс
16.	Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. — 3-е изд. — Москва : РИОР : ИНФРА-М, 2021. — 400 с. — (Высшее образование). — DOI: https://doi.org/10.12737/1759-3. - ISBN 978-5-369-01759-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1210523 (дата обращения: 16.07.2021). – Режим доступа: по подписке.	Электронный ресурс
17.	Комарова, В. В. Управление проектами : учебное пособие / В. В. Комарова. — Хабаровск : ДВГУПС, 2020. — 158 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/179375 (дата обращения: 06.079.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
18.	Кравцова, Е. Д. Логика и методология научных исследований : учеб. пособие / Е. Д. Кравцова, А. Н. Городищева. - Красноярск : Сиб. федер. ун-т, 2014. - 168 с. - ISBN 978-5-7638-2946-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/507377 (дата обращения: 06.07.2021). – Режим доступа: по подписке.	Электронный ресурс
19.	Краковский, Ю. М. Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/156401 (дата обращения: 07.07.2021). — Режим доступа: для авториз. пользователей.	
20.	Куняев, Н. Н. Правовое обеспечение национальных интересов Российской Федерации в информационной сфере : монография / Н. Н. Куняев. - Москва : Логос, 2020. - 348 с. - ISBN 978-5-98704-513-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/1213114 (дата обращения: 06.07.2021). – Режим доступа: по подписке.	Электронный ресурс
21.	Малюк, А. А. Защита информации в информационном обществе [Электронный ресурс] : учеб. пособие / А. А. Малюк. – М. : Горячая линия-Телеком, 2017. – 230 с. – Режим доступа: https://e.lanbook.com/book/111078 – Загл. с экрана	50
22.	Методология научного исследования : учебник для вузов / Н. А. Слесаренко, Е. Н. Борхунова, С. М. Борунова [и др.] ; под редакцией Н. А. Слесаренко. — 5-е изд., стер. — Санкт-Петербург : Лань, 2021. — 268 с. — ISBN 978-5-8114-7204-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/156383 (дата обращения: 06.07.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
23.	Мошак, Н. Н. Защищенные информационные системы : учебное пособие / Н. Н. Мошак, Л. К. Птицына. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2020. — 216 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/180099 (дата обращения: 06.07.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
24.	Нестеров, С. А. Основы информационной безопасности : учебник для вузов / С. А. Нестеров. — Санкт-Петербург : Лань, 2021. — 324 с. — ISBN 978-5-8114-6738-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/165837 (дата обращения: 16.07.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
25.	Овчаров, А. О. Методология научного исследования : учебник / А.О. Ов-	Электронный

	чаров, Т.Н. Овчарова. — Москва : ИНФРА-М, 2021. — 304 с. + Доп. материалы [Электронный ресурс]. — (Высшее образование: Магистратура). — DOI 10.12737/357. - ISBN 978-5-16-009204-1. - Текст : электронный. - URL: https://znanium.com/catalog/product/1545403 (дата обращения: 06.07.2021). – Режим доступа: по подписке.	ресурс
26.	Основы перевода, аннотирования и реферирования научно-технического текста : учебное пособие / Е. А. Чигирин, Т. Ю. Чигирина, Я. А. Ковалевская, Е. В. Козыренко. — Воронеж : ВГУИТ, 2019. — 154 с. — ISBN 978-5-00032-437-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/143274 (дата обращения: 19.07.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
27.	Павлова, Р. С. Документационное обеспечение управления : учебник для вузов / Р. С. Павлова. — Санкт-Петербург : Лань, 2021. — 416 с. — ISBN 978-5-8114-6960-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/173088 (дата обращения: 06.07.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
28.	Пелешенко, В. С. Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления : учебное пособие / В. С. Пелешенко, С. В. Говорова, М. А. Лапина. — Ставрополь : СКФУ, 2017. — 86 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/155146 (дата обращения: 20.07.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
29.	Попов, Р. А. Современные системы управления деятельностью : учебник / Р. А. Попов. — Москва : ИНФРА-М, 2021. — 309 с. — (Высшее образование: Магистратура). - ISBN 978-5-16-016191-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/1150849 (дата обращения: 06.07.2021). – Режим доступа: по подписке.	Электронный ресурс
30.	Преображенская, Т. В. Управление проектами : учебное пособие / Т. В. Преображенская, М. Ш. Муртазина, А. А. Алетдинова. — Новосибирск : НГТУ, 2018. — 123 с. — ISBN 978-5-7782-3558-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/118241 (дата обращения: 06.07.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
31.	Проскурин, В. Г. Защита в операционных системах : учебное пособие / В. Г. Проскурин. — Москва : Горячая линия-Телеком, 2016. — 192 с. — ISBN 978-5-9912-0379-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111091 (дата обращения: 06.07.2021). — Режим доступа: для авториз. пользователей.	
32.	Риск-контроллинг информационной и экономической безопасности : монография / Г. И. Золотарева, С. В. Филько, И. В. Филько, И. В. Федоренко. — Красноярск : СибГУ им. академика М. Ф. Решетнёва, 2018. — 192 с. — ISBN 978-5-86433-759-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/147582 (дата обращения: 06.07.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
33.	Сертификация средств защиты информации : учебное пособие / А. А. Миняев, Юркин, М. М. Ковцур, К. А. Ахрамееева. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2020. — 88 с. — ISBN 978-5-89160-213-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/180100 (дата обращения: 06.07.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
34.	Трухин, М. П. Моделирование сигналов и систем. Основы разработки компьютерных моделей систем и сигналов : учебное пособие для вузов / М. П. Трухин. — 2-е изд., стер. — Санкт-Петербург : Лань, 2021. — 212 с.	Электронный ресурс

	— ISBN 978-5-8114-8064-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/171422 (дата обращения: 06.07.2021). — Режим доступа: для авториз. пользователей.	
35.	Управление проектами : учебник / В. Н. Островская, Г. В. Воронцова, О. Н. Момотова [и др.]. — Санкт-Петербург : Лань, 2018. — 400 с. — ISBN 978-5-8114-2818-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/103076 (дата обращения: 06.07.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
36.	Шаньгин, В. Ф. Защита компьютерной информации : учебное пособие / В. Ф. Шаньгин. — Москва : ДМК Пресс, 2010. — 544 с. — ISBN 978-5-94074-518-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/1122 (дата обращения: 06.07.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс

7.2 Дополнительная литература

№ п/п	Библиографическое описание	Количество экземпляров в библиотеке СГУГиТ
1.	Андрианова, Е. Г. Информационные системы управления ресурсами предприятия : методические рекомендации / Е. Г. Андрианова. — Москва : РТУ МИРЭА, 2020. — 63 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/167615 (дата обращения: 06.07.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
2.	Аникин, Д. В. Информационная безопасность и защита информации : учебное пособие / Д. В. Аникин. — Санкт-Петербург : ИЭО СПбУТУиЭ, 2011. — 269 с. — ISBN 978-5-94047-394-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/63950 (дата обращения: 06.07.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
3.	Баранова, Е. К. Актуальные вопросы защиты информации : монография / А.В. Бабаш, Е.К. Баранова. — Москва : РИОР : ИНФРА-М, 2021. — 111 с. — (Научная мысль). — https://doi.org/10.12737/monography_58dbc380aa3a4. - ISBN 978-5-369-01680-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1282721 (дата обращения: 15.07.2021). – Режим доступа: по подписке.	Электронный ресурс
4.	Баранова, Е. К. Актуальные вопросы защиты информации : монография / А.В. Бабаш, Е.К. Баранова. — Москва : РИОР : ИНФРА-М, 2021. — 111 с. — (Научная мысль). — https://doi.org/10.12737/monography_58dbc380aa3a4. - ISBN 978-5-369-01680-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1282721 (дата обращения: 15.07.2021). – Режим доступа: по подписке.	Электронный ресурс
5.	Батоврин, В. К. Управление жизненным циклом технических систем на основе современных стандартов : учебное пособие / В. К. Батоврин, А. С. Королев. — Москва : НИЯУ МИФИ, 2016. — 92 с. — ISBN 978-5-7262-2201-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/119498 (дата обращения: 06.07.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс

6.	Бедердинова, О. И. Автоматизированное управление IT-проектами : учебное пособие / О.И. Бедердинова, Ю.А. Водовозова. — Москва : ИНФРА-М, 2021. — 92 с. - ISBN 978-5-16-109404-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/1242887 (дата обращения: 06.09.2021)	Электронный ресурс
7.	Веселов, Г. Е. Менеджмент риска информационной безопасности: Учебное пособие / Веселов Г.Е., Абрамов Е.С., Шилов А.К. - Таганрог:Южный федеральный университет, 2016. - 107 с.: ISBN 978-5-9275-2327-5. - Текст : электронный. - URL: https://znanium.com/catalog/product/997108 (дата обращения: 20.07.2021). – Режим доступа: по подписке.	Электронный ресурс
8.	Ворона, В. А. Системы контроля и управления доступом / В. А. Ворона, В. А. Тихонов. — Москва : Горячая линия-Телеком, 2018. — 272 с. — ISBN 978-5-9912-0059-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111037 (дата обращения: 06.07.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
9.	Вотинов, М. В. Хранение и защита компьютерной информации : учебное пособие / М. В. Вотинов. — Мурманск : МГТУ, 2017. — 82 с. — ISBN 978-5-86185-947-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/142646 (дата обращения: 20.07.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
10.	Гвоздева, Т. В. Проектирование информационных систем. Стандартизация [Электрон-ный ресурс] : учеб. пособие / Т. В. Гвоздева, Б. А. Баллод. – СПб. : Лань, 2019. – 252 с. – Режим доступа: https://e.lanbook.com/book/115515 – Загл. с экрана	Электронный ресурс
11.	Гультяева, Т. А. Основы защиты информации : учебное пособие / Т. А. Гультяева. — Новосибирск : НГТУ, 2018. — 83 с. — ISBN 978-5-7782-3641-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/118234 (дата обращения: 07.07.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
12.	Данилов, А. Н. Основы информационной безопасности : учебное пособие / А. Н. Данилов, С. А. Данилова, А. А. Зорин. — Пермь : ПНИПУ, 2008. — 556 с. — ISBN 978-5-398-00132-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/160787 (дата обращения: 06.07.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
13.	Дудяшова, В. П. Методология научных исследований : учебное пособие / В. П. Дудяшова. — Кострома : КГУ им. Н.А. Некрасова, 2021. — 80 с. — ISBN 978-5-8285-1132-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/177619 (дата обращения: 06.07.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
14.	Зайцев, А. П. Технические средства и методы защиты информации : учебник / А. П. Зайцев, Р. В. Мещеряков, А. А. Шелупанов. — 7-е изд., испр. — Москва : Горячая линия-Телеком, 2018. — 442 с. — ISBN 978-5-9912-0233-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111057 (дата обращения: 07.07.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
15.	Иванова, Н. В. Применение интеллектуальных систем: практикум по выполнению лабораторных работ : учебное пособие / Н. В. Иванова, А. М. Перепеченов. — Санкт-Петербург : ПГУПС, 2019. — 47 с. — ISBN 978-5-7641-1361-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/171840 (дата обращения: 07.07.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс

16.	Казаков, Ю. В. Системный подход к научно-исследовательской работе : учебное пособие / Ю. В. Казаков. — Тольятти : ТГУ, 2010. — 68 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/139737 (дата обращения: 19.07.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
17.	Каширин, И. Ю. Автоматизированный анализ деятельности предприятия с использованием семантических сетей : монография / И. Ю. Каширин, А. В. Крошилин, С. В. Крошилина. — Москва : Горячая линия-Телеком, 2013. — 140 с. — ISBN 978-5-9912-0171-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111062 (дата обращения: 06.07.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
18.	Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва : ИНФРА-М, 2021. — 180 с. — (Научная мысль). — DOI 10.12737/monography_5d412ff13c0b88.75804464. - ISBN 978-5-16-015149-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1137902 (дата обращения: 15.07.2021). – Режим доступа: по подписке.	Электронный ресурс
19.	Ковалев, Д. В. Информационная безопасность: Учебное пособие / Ковалев Д.В., Богданова Е.А. - Ростов-на-Дону:Южный федеральный университет, 2016. - 74 с.: ISBN 978-5-9275-2364-1. - Текст : электронный. - URL: https://znanium.com/catalog/product/997105 (дата обращения: 15.07.2021). – Режим доступа: по подписке.	Электронный ресурс
20.	Коваленко, Ю. И. Правовой режим лицензирования и сертификации в сфере информационной безопасности : учебное пособие / Ю. И. Коваленко. — Москва : Горячая линия-Телеком, 2012. — 140 с. — ISBN 978-5-9912-0261-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/5163 (дата обращения: 06.07.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
21.	Крюков, С. В. Системный анализ: теория и практика: учеб. пособие / Крюков С.В. - Ростов-на-Дону:Издательство ЮФУ, 2011. - 228 с. ISBN 978-5-9275-0851-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/556278 (дата обращения: 15.07.2021). – Режим доступа: по подписке.	Электронный ресурс
22.	Курило, А. П. Основы управления информационной безопасностью. Серия «Вопросы управления информационной безопасностью". Выпуск 1 [Электронный ресурс] / А. П. Курило, Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. – М. : Горячая линия-Телеком, 2012. – 244 с. – Режим доступа: http://e.lanbook.com/book/5178 – Загл. с экрана.	Электронный ресурс
23.	Малюк, А. А. Теория защиты информации / А. А. Малюк. — Москва : Горячая линия-Телеком, 2015. — 184 с. — ISBN 978-5-9912-0246-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111077 (дата обращения: 19.07.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
24.	Методология научного исследования : учебник для вузов / Н. А. Слесаренко, Е. Н. Борхунова, С. М. Борунова [и др.] ; под редакцией Н. А. Слесаренко. — 5-е изд., стер. — Санкт-Петербург : Лань, 2021. — 268 с. — ISBN 978-5-8114-7204-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/156383 (дата обращения: 06.07.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
25.	Методы защищенного управления информационнообразовательными фондами вузов : монография / С. Г. Фомичева, С. В. Беззатеев, Т. Н. Ели-	Электронный ресурс

	на, А. А. Попкова. — Норильск : НГИИ, 2012. — 208 с. — ISBN 978-5-89009-538-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/155903 (дата обращения: 06.07.2021). — Режим доступа: для авториз. пользователей.	
26.	Милославская, Н. Г. Проверка и оценка деятельности по управлению информационной безопасностью. Серия «Вопросы управления информационной безопасностью". Выпуск 5 [Электронный ресурс] : учеб. пособие / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. – М. : Горячая линия-Телеком, 2012. – 166 с. – Режим доступа: https://e.lanbook.com/book/5182 – Загл. с экрана.	Электронный ресурс
27.	Милославская, Н. Г. Серия «Вопросы управление информационной безопасностью". Выпуск 3 : учебное пособие / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. — Москва : Горячая линия-Телеком, 2013. — 170 с. — ISBN 978-5-9912-0273-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/5180 (дата обращения: 10.07.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
28.	Милославская, Н. Г. Управление рисками информационной безопасности. Серия «Вопросы управления информационной безопасностью". Выпуск 2 [Электронный ресурс] / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. – М. : Горячая линия-Телеком, 2012. – 130 с. – Режим доступа: http://e.lanbook.com/book/5179 – Загл. с экрана.	Электронный ресурс
29.	Моргунов, А. В. Информационная безопасность : учебно-методическое пособие / А. В. Моргунов. — Новосибирск : НГТУ, 2019. — 83 с. — ISBN 978-5-7782-3918-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/152227 (дата обращения: 07.07.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
30.	Организация и проведение научно-исследовательской работы магистрантов [Текст] : метод. указания / В. А. Павленко, Ю. Ю. Соловьева, Е. И. Аврунев ; СГГА. – Новосибирск : СГГА, 2014. – 16, [1] с.	Электронный ресурс
31.	Основы информационной безопасности : учебное пособие / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. — Москва : Горячая линия-Телеком, 2011. — 558 с. — ISBN 5-93517-292-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111016 (дата обращения: 20.07.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
32.	Основы управления информационной безопасностью. Серия «Вопросы управление информационной безопасностью". Выпуск 1 : учебное пособие / А. П. Курило, Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. — Москва : Горячая линия-Телеком, 2012. — 244 с. — ISBN 978-5-9912-0271-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/5178 (дата обращения: 16.07.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
33.	Остроух, А. В. Интеллектуальные информационные системы и технологии [Электрон-ный ресурс] : монография / А. В. Остроух, А. Б. Николаев. – СПб. : Лань, 2019. – 308 с. – Режим доступа: https://e.lanbook.com/book/115518 – Загл. с экрана	Электронный ресурс
34.	Пелешенко, В. С. Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления : учебное пособие / В. С. Пелешенко, С. В. Говорова, М. А. Лапина. — Ставрополь : СКФУ, 2017. — 86 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/155146 (дата обращения: 19.07.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс

35.	Петров, А. А. Компьютерная безопасность. Криптографические методы защиты / А. А. Петров. — Москва : ДМК Пресс, 2008. — 448 с. — ISBN 5-89818-064-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/3027 (дата обращения: 06.07.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
36.	Поддержка принятия решений при проектировании систем защиты информации : монография / В.В. Бухтояров, М.Н. Жукова, В.В. Золотарев [и др.]. — Москва : ИНФРА-М, 2020. — 131 с. — (Научная мысль). — www.dx.doi.org/10.12737/2248. - ISBN 978-5-16-009519-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1036519 (дата обращения: 16.07.2021). – Режим доступа: по подписке.	Электронный ресурс
37.	Правовое регулирование информационных отношений в области государственной и коммерческой тайны, персональных данных : учебное пособие / О. В. Ахрамеева, И. Ф. Дедюхина, О. В. Жданова, Н. В. Мирошниченко. — Ставрополь : СтГАУ, 2015. — 59 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/82255 (дата обращения: 06.07.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
38.	Проектирование, разработка и обеспечение безопасности информационных систем : монография / В. В. Бабенко, Р. А. Гашин, Ю. В. Гольчевский [и др.]. — Сыктывкар : СГУ им. Питирима Сорокина, 2016. — 146 с. — ISBN 978-5-87661-395-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/176919 (дата обращения: 06.07.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
39.	Проскурин, В. Г. Защита в операционных системах : учебное пособие / В. Г. Проскурин. — Москва : Горячая линия-Телеком, 2016. — 192 с. — ISBN 978-5-9912-0379-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111091 (дата обращения: 06.07.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
40.	Ренгольд, О. В. Методология научных исследований : учебно-методическое пособие / О. В. Ренгольд. — Омск : СибАДИ, 2019. — 46 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/149506 (дата обращения: 06.07.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
41.	Риск и рефлексия : монография / В. П. Балан, С. А. Баркалов, А. В. Душкин [и др.] ; под общей редакцией В. И. Новосельцева. — Москва : Горячая линия-Телеком, 2016. — 136 с. — ISBN 978-5-9912-0590-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/107645 (дата обращения: 20.07.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
42.	Сабанов, А. Г. Защита персональных данных в организациях здравоохранения : учебное пособие / А. Г. Сабанов, В. Д. Зыков, Р. В. Мещеряков. — Москва : Горячая линия-Телеком, 2012. — 206 с. — ISBN 978-5-9912-0243-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/5194 (дата обращения: 20.07.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
43.	Сертификация средств защиты информации : учебное пособие / А. А. Миняев, Юркин, М. М. Ковцур, К. А. Ахрамееева. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2020. — 88 с. — ISBN 978-5-89160-213-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/180100 (дата обращения: 06.07.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
44.	Теоретические основы управления в организациях [Электронный ресурс]	Электронный

	: учеб. пособие / В. П. Балан, А. В. Душкин, В. И. Новосельцев, В. И. Сумин ; под редакцией В. И. Новосельцев. – М. : Горячая линия-Телеком, 2016. – 244 с. – Режим доступа: https://e.lanbook.com/book/107634 – Загл. с экрана	ресурс
45.	Тихомирова, О. Г. Управление проектом: комплексный подход и системный анализ : монография / О.Г. Тихомирова. — Москва : ИНФРА-М, 2022. — 300 с. — (Научная мысль). — DOI 10.12737/673. - ISBN 978-5-16-006383-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1709593 (дата обращения: 15.07.2021). – Режим доступа: по подписке.	Электронный ресурс
46.	Тишина, Н. А. Прикладные задачи безопасности информационно-телекоммуникационных систем : учебное пособие / Н. А. Тишина, Е. Н. Чернопрудова. — Оренбург : ОГУ, 2017. — 122 с. — ISBN 978-5-7410-1892-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/110630 (дата обращения: 06.07.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
47.	Управление качеством систем менеджмента информационной безопасности : учебное пособие / А. В. Красов, И. И. Лившиц, Д. В. Юркин, А. В. Малых. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2016. — 74 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/180090 (дата обращения: 06.07.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
48.	Управление проектами : учеб. пособие / П.С. Зеленский, Т.С. Зимнякова, Г.И. Поподько (отв. ред.) [и др.]. - Красноярск : Сиб. федер. ун-т, 2017. - 125 с. - ISBN 978-5-7638-3711-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/1031863 (дата обращения: 06.07.2021). – Режим доступа: по подписке.	Электронный ресурс
49.	Царенко, А. С. Управление проектами : учебное пособие для вузов / А. С. Царенко. — Санкт-Петербург : Лань, 2021. — 236 с. — ISBN 978-5-8114-7568-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/176880 (дата обращения: 06.07.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
50.	Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях : учебное пособие / В. Ф. Шаньгин. — Москва : ДМК Пресс, 2012. — 592 с. — ISBN 978-5-94074-637-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/3032 (дата обращения: 06.07.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
51.	Шаньгин, В. Ф. Информационная безопасность : учебное пособие / В. Ф. Шаньгин. — Москва : ДМК Пресс, 2014. — 702 с. — ISBN 978-5-94074-768-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/50578 (дата обращения: 06.07.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
52.	Шариков, П. А. Проблемы информационной безопасности в полицентричном мире / П.А. Шариков. - М.: Весь Мир, 2015. - 320 с. ISBN 978-5-7777-0601-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1013794 (дата обращения: 20.07.2021). – Режим доступа: по подписке.	Электронный ресурс
53.	Шерстюк, Н. Э. Методические указания по выполнению выпускной квалификационной работы магистра (магистерской диссертации) : методические указания / Н. Э. Шерстюк, И. В. Гладышев, В. В. Кузнецов. — 2-е изд. испр. — Москва : РТУ МИРЭА, 2021. — 44 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/176574 (дата обращения: 19.07.2021). — Режим	Электронный ресурс

	доступа: для авториз. пользователей.	

7.3 Нормативная документация

1 Стратегия национальной безопасности Российской Федерации до 2020 года Утверждена Указом Президента Российской Федерации от 12 мая 2009 г. N 537 http://www.fstec.ru.

2 Доктрина информационной безопасности Российской Федерации: утв. Президентом РФ В. В. Путиным 5 декабря. 2016 г. Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. №646 // Российская газета. – 2016, 06.12.2016.

3 Федеральный закон N 127-ФЗ от 23 августа 1996 г «О науке и государственной научно-технической политике» (с изменениями и дополнениями);

4 Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ;

5 Федеральный государственный образовательный стандарт высшего образования по направлению подготовки 10.04.01 Информационная безопасность (уровень магистратуры).

6 Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» // СПС Консультант+.

7 Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне» (в ред. Федеральных законов от 02.02.2006 №19ФЗ, от 18.12.2006 № 231-ФЗ, от 24.07.2007 № 214-ФЗ) // СПС Консультант+.

8 Закон РФ «О государственной тайне» от 21 июня 1993 г. № 5485-I // СПС Консультант+.

9 Указ Президента РФ от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» // СПС Консультант+.

10 Постановление Правительства Российской Федерации от 04.09.95 № 870 “Правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности” // СПС Консультант+.

11 Гражданский кодекс РФ // СПС Консультант+.

12 Иностранная техническая компьютерная разведка. Приложение № 2 к Модели иностранных технических разведок на период до 2025 года (Модель ИТР-2025), утвержденной приказом ФСТЭК России от 01.12.2015 № 047 и введенной в действие с 01.06.2016 г.

13 Иностранные технические средства наблюдения и контроля. Приложение № 1 к Модели иностранных технических разведок на период до 2025 года (Модель ИТР-2025), утвержденной приказом ФСТЭК России от 01.12.2015 № 047 и введенной в действие с 01.06.2016 г.

14 Иностранные технические средства разведки стационарных объектов органов государственной власти, органов местного самоуправления и организаций. Приложение № 4 к Модели иностранных технических разведок на период до 2025 года (Модель ИТР-2025), утвержденной приказом ФСТЭК России от 01.12.2015 № 047 и введенной в действие с 01.06.2016 г.

15 Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждено ФСТЭК России 15.02.2008.

16 Методика оценки эффективности защиты информации, обрабатываемой объектами вычислительной техники, от утечки за счет побочных электромагнитных излучений и наводок (ПЭМИН). Утверждена приказом ФСТЭК России от 27.11.2017 № 043.

17 Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждено ФСТЭК России 25.12.2006.

18 Основные мероприятия по организации и обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных. Утверждено ФСТЭК России 15.02.2008.

19 Перечень сведений, подлежащих засекречиванию, Министерства образования и науки Российской Федерации. Раздел VI. Сведения в области защиты государственной тайны. Утверждены приказом Минобрнауки России от 10.11.2014 № 36с, действие продлено приказом Минобрнауки России от 20.12.2019 № 51/гт.

20 Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждено ФСТЭК России 15.02.2008.

21 Типовая инструкция по обеспечению режима секретности при обработке секретной информации (по обеспечению безопасности информации) с использованием СВТ. Одобрена решением МКЗГТ от 09.10.2009 № 172.

22 Требования к средствам антивирусной защиты. Утверждены приказом ФСТЭК России от 20.03.2012 № 28. Инв. № 891.

23 Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждено ФСТЭК России 15.02.2008.

24 ГОСТ Р 57102-2016 Информационные технологии. Системная и программная инженерия. Часть 2. Руководство по применению ИСО/МЭК 15288.

25 ГОСТ Р 58256-2018 Управление потоками информации в информационной системе. Формат классификационных меток.

26 ГОСТ Р 58833-2020 Защита информации. Идентификация и аутентификация. Общие положения.

27 ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации

28 ГОСТ Р ИСО/МЭК 12207-2010 Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств.

29 ГОСТ Р ИСО/МЭК 27005-2010 Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. – М.: Стандартинформ, 2011. – 51 с.;

30 ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Методы и средства обеспечения. безопасности. Часть 3. Методы менеджмента безопасности информационных технологий.

31 ГОСТ РО 0043-003-2012 Защита информации. Аттестация объектов информатизации. Общие положения. ДСП.

32 Государственная итоговая аттестация выпускников СГУГиТ. Структура и правила оформления [Электронный ресурс]: СТО СМК СГУГиТ 8-06-2021. - Новосибирск : СГУГиТ, 2021. - 69 с. – Режим доступа: http://lib.sgugit.ru –Загл. с экрана.

33 ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования.

34 ГОСТ Р 50922-2006 Защита информации. Основные термины и определения.

7.4 Периодические издания

1. Журнал «Защита информации. Инсайд»;
2. Журнал «Information Security»;
3. Журнал «Информация и безопасность»;
4. Журнал «Информационная безопасность регионов».

7.5 Электронно-библиотечные системы, современные профессиональные базы данных и информационные справочные системы

Обучающиеся обеспечены доступом (удаленным доступом), в том числе в случае применения электронного обучения, дистанционных образовательных технологий, к современным профессиональным базам данных и информационным справочным системам:

1. Сетевые локальные ресурсы (авторизованный доступ для работы с полнотекстовыми документами, свободный доступ в остальных случаях). – Режим доступа: http://lib.sgugit.ru.

2. Сетевые удалённые ресурсы:

– электронно-библиотечная система издательства «Лань». – Режим доступа: http://e.lanbook.com (получение логина и пароля с компьютеров СГУГиТ, дальнейший авторизованный доступ с любого компьютера, подключенного к интернету);

– электронно-библиотечная система Znanium.com. – Режим доступа: http://znanium.com (доступ по логину и паролю с любого компьютера, подключенного к интернету);

- научная электронная библиотека elibrary. – Режим доступа: http://www.elibrary.ru (доступ с любого компьютера, подключенного к интернету);

– электронная информационно-справочная система «Техэксперт». – Режим доступа: http://bnd2.kodeks.ru/kodeks01/ (доступ по логину и паролю с любого компьютера, подключенного к интернету).

3. Электронная справочно-правовая система (база данных) «КонсультантПлюс». – Режим доступа: http://www.consultant.ru

4. Национальная электронная библиотека (НЭБ). – Режим доступа: http://www.rusneb.ru (доступ с любого компьютера, подключенного к интернету).