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, 2022

Программа государственной итоговой аттестации по направлению подготовки магистров *10.04.01 Информационная безопасность* составлена на основании федерального государственного образовательного стандарта высшего образования, утвержденного приказом Министерства образования и науки Российской Федерации от 01 декабря 2016 г. № 1513 и учебного плана профиля «*Организация и управление информационной безопасностью*» (магистратура).

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 (ИБ)*

Зам. зав. кафедрой ИБ _____ *А.В. Троеглазова*
(подпись)

Программа одобрена ученым советом *Института оптики и технологий информационной безопасности (ИОиТИБ)*

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 обучения – на 3 курсе.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

3.1. Перечень компетенций, которыми должны овладеть обучающиеся в результате освоения образовательной программы

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

Таблица 1

Перечень компетенций

Код компетенции	Содержание формируемой компетенции	Уровни сформированности компетенции	Образовательные результаты	Шкала оценивания
ОК-1	Способностью к абстрактному мышлению, анализу, синтезу	ПОВЫШЕННЫЙ	*Выпускник знает:* на высоком уровне основные подходы и методы управления проектами; методы анализа и синтеза информации; методы научного исследования путём мысленного расчленения объекта (анализ) и путём изучения предмета в его целостности, единстве его частей (синтез). *Выпускник умеет:* на высоком уровне самостоятельности абстрактно мыслить; анализировать и обобщать полученную в ходе исследования информацию; выявлять и оценивать проблемы, возникающие в ходе реализации проекта; использовать методы абстрактного мышления, анализа и синтеза; выявлять альтернативные варианты решения исследовательских задач. *Выпускник владеет:* с высокой адаптивностью практического навыка способностью к абстрактному мышлению, анализу и синтезу; навыками и опытом разработки структурной модели проекта; целостной системой навыков использования абстрактного мышления при решении проблем.	5
		БАЗОВЫЙ	*Выпускник знает:* на достаточном уровне основные подходы и методы управления проектами; методы анализа и синтеза информации; методы научного исследования путём мысленного расчленения объекта (анализ) и путём изучения предмета в его целостности, единстве его частей (синтез).	4

			Выпускник умеет: на достаточном уровне самостоятельности абстрактно мыслить; анализировать и обобщать полученную в ходе исследования информацию; выявлять и оценивать проблемы, возникающие в ходе реализации проекта; использовать методы абстрактного мышления, анализа и синтеза; выявлять альтернативные варианты решения исследовательских задач. *Выпускник владеет:* с достаточной адаптивностью практического навыка способностью к абстрактному мышлению, анализу и синтезу; навыками и опытом разработки структурной модели проекта; целостной системой навыков использования абстрактного мышления при решении проблем.	
		ПОРОГОВЫЙ	*Выпускник знает:* на допустимом уровне основные подходы и методы управления проектами; методы анализа и синтеза информации; методы научного исследования путём мысленного расчленения объекта (анализ) и путём изучения предмета в его целостности, единстве его частей (синтез). *Выпускник умеет:* на допустимом уровне самостоятельности абстрактно мыслить; анализировать и обобщать полученную в ходе исследования информацию; выявлять и оценивать проблемы, возникающие в ходе реализации проекта; использовать методы абстрактного мышления, анализа и синтеза; выявлять альтернативные варианты решения исследовательских задач. *Выпускник владеет:* с допустимой адаптивностью практического навыка способностью к абстрактному мышлению, анализу и синтезу; навыками и опытом разработки структурной модели проекта; целостной системой навыков использования абстрактного мышления при решении проблем.	3
ОК-2	Способностью самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности	ПОВЫШЕННЫЙ	*Выпускник знает:* на высоком уровне современные операционные системы, принцип работы; основные функции операционных систем; сопровождение операционных систем; теоретические, методические и организационные аспекты осуществления научно-исследовательской деятельности, методологию научно-исследовательской деятель-	5

	новые знания и умения		ности в образовании; особенности диссертационного исследования как вида научно-исследовательской работы. *Выпускник умеет:* на высоком уровне самостоятельности использовать средства операционных систем и сред для решения практических задач; оценивать эффективность и надежность защиты ОС; применять теоретические знания по методам сбора, хранения, обработки, передачи и защиты информации с использованием современных информационных технологий, средства и методы научного исследования. *Выпускник владеет:* навыками построения защиты ОС Windows, Unix; навыками планирования научного исследования, анализа получаемых результатов и формулировки выводов; спецификой научно-исследовательской работы с высокой адаптивностью практического навыка	
		БАЗОВЫЙ	*Выпускник знает:* на достаточном уровне современные операционные системы, принцип работы; основные функции операционных систем; сопровождение операционных систем; теоретические, методические и организационные аспекты осуществления научно-исследовательской деятельности, методологию научно-исследовательской деятельности в образовании; особенности диссертационного исследования как вида научно-исследовательской работы. *Выпускник умеет:* на достаточном уровне самостоятельности использовать средства операционных систем и сред для решения практических задач; оценивать эффективность и надежность защиты ОС; применять теоретические знания по методам сбора, хранения, обработки, передачи и защиты информации с использованием современных информационных технологий, средства и методы научного исследования. *Выпускник владеет:* навыками построения защиты ОС Windows, Unix; навыками планирования научного исследования, анализа получаемых результатов и формулировки выводов; спецификой научно-	4

			исследовательской работы с достаточной адаптивностью практического навыка.	
		ПОРОГОВЫЙ	*Выпускник знает:* на допустимом уровне современные операционные системы, принцип работы; основные функции операционных систем; сопровождение операционных систем; теоретические, методические и организационные аспекты осуществления научно-исследовательской деятельности, методологию научно-исследовательской деятельности в образовании; особенности диссертационного исследования как вида научно-исследовательской работы. *Выпускник умеет:* на допустимом уровне самостоятельности использовать средства операционных систем и сред для решения практических задач; оценивать эффективность и надежность защиты ОС; применять теоретические знания по методам сбора, хранения, обработки, передачи и защиты информации с использованием современных информационных технологий, средства и методы научного исследования. *Выпускник владеет:* навыками построения защиты ОС Windows, Unix; навыками планирования научного исследования, анализа получаемых результатов и формулировки выводов; спецификой научно-исследовательской работы с допустимой адаптивностью практического навыка.	3
ОПК-1	Способностью к коммуникации в устной и письменной формах на государственном и одном из иностранных языков для решения задач профессиональной деятельности	ПОВЫШЕННЫЙ	*Выпускник знает:* на высоком уровне базовые правила грамматики (на уровне морфологии и синтаксиса), базовые нормы употребления лексики и фонетики; основные нормы языка (орфографические, пунктуационные, грамматические, стилистические, орфоэпические) и систему функциональных стилей. *Выпускник умеет:* на высоком уровне самостоятельности понимать основное содержание несложных аутентичных общественно-политических, публицистических и прагматических текстов (информационных буклетов, брошюр/проспектов), научно-популярных и научных текстов, блогов/веб-сайтов; выделять значимую/запрашиваемую информацию из прагматических текстов справочно-информационного и рекламного характера;	5

			пользоваться основной справочной литературой, толковыми и нормативными словарями. *Выпускник владеет:* приемами самостоятельной работы с языковым материалом (лексикой, грамматикой, фонетикой) с использованием справочной и учебной литературы; приемами самостоятельной работы с языковым материалом (лексикой, грамматикой, фонетикой) с использованием справочной и учебной литературы с высокой адаптивностью практического навыка.	
		БАЗОВЫЙ	*Выпускник знает:* на достаточном уровне базовые правила грамматики (на уровне морфологии и синтаксиса), базовые нормы употребления лексики и фонетики; основные нормы языка (орфографические, пунктуационные, грамматические, стилистические, орфоэпические) и систему функциональных стилей. *Выпускник умеет:* на достаточном уровне самостоятельности понимать основное содержание несложных аутентичных общественно-политических, публицистических и прагматических текстов (информационных буклетов, брошюр/проспектов), научно-популярных и научных текстов, блогов/веб-сайтов; выделять значимую/запрашиваемую информацию из прагматических текстов справочно-информационного и рекламного характера; пользоваться основной справочной литературой, толковыми и нормативными словарями. *Выпускник владеет:* приемами самостоятельной работы с языковым материалом (лексикой, грамматикой, фонетикой) с использованием справочной и учебной литературы; приемами самостоятельной работы с языковым материалом (лексикой, грамматикой, фонетикой) с использованием справочной и учебной литературы с достаточной адаптивностью практического навыка.	4
		ПОРОГОВЫЙ	*Выпускник знает:* на допустимом уровне базовые правила грамматики (на уровне морфологии и синтаксиса), базовые нормы употребления лексики и фонетики; основные нормы языка (орфографические, пунктуационные,	3

			грамматические, стилистические, орфоэпические) и систему функциональных стилей. *Выпускник умеет:* на допустимом уровне самостоятельности понимать основное содержание несложных аутентичных общественно-политических, публицистических и прагматических текстов (информационных буклетов, брошюр/проспектов), научно-популярных и научных текстов, блогов/веб-сайтов; выделять значимую/запрашиваемую информацию из прагматических текстов справочно-информационного и рекламного характера; пользоваться основной справочной литературой, толковыми и нормативными словарями**.** *Выпускник владеет:* приемами самостоятельной работы с языковым материалом (лексикой, грамматикой, фонетикой) с использованием справочной и учебной литературы; приемами самостоятельной работы с языковым материалом (лексикой, грамматикой, фонетикой) с использованием справочной и учебной литературы с допустимой адаптивностью практического навыка.	
ОПК-2	Способностью к самостоятельному обучению и применению новых методов исследования профессиональной деятельности	ПОВЫШЕННЫЙ	*Выпускник знает:* на высоком уровне основные научные направления развития науки и техники в профессиональной области деятельности; критерии оценки эффективности и надежности средств защиты ОС; основы методологии науки, научные парадигмы, методы научных исследований в смежных областях; эффективные способы освоения и использования новых методов исследования и применения их в новых сферах профессиональной деятельности. *Выпускник умеет:* на высоком уровне анализировать состояние научно-технической проблемы в профессиональной области деятельности и на этой основе определить цель исследования, методы и средства ее реализации; выбирать и создавать критерии оценки исследований; пользоваться средствами защиты, предоставляемыми ОС; структурировать научное знание, применять современные методы исследований, оценивать и представлять их результаты, аргументировано их защищать; структурировать науч-	5

			ное знание, применять современные методы исследований, оценивать и представлять их результаты, аргументировано их защищать; осваивать и использовать новые методы исследования и применять их в новых сферах профессиональной деятельности. *Выпускник владеет:* приёмами прогнозирования тенденций развития науки и техники в профессиональной области деятельности; навыками выбора и создания критериев оценки исследований; навыками администрирования операционных систем; опытом выполнения исследований современными методами в области оптической техники, оптико-электронных приборов и систем, навыками обработки, анализа научных результатов и их представления в наглядном виде; способностью к самостоятельному освоению и использованию новых методов исследования и применения их в новых сферах профессиональной деятельности с высокой адаптивностью практического навыка.	
		БАЗОВЫЙ	*Выпускник знает:* на достаточном уровне основные научные направления развития науки и техники в профессиональной области деятельности; критерии оценки эффективности и надежности средств защиты ОС; основы методологии науки, научные парадигмы, методы научных исследований в смежных областях; эффективные способы освоения и использования новых методов исследования и применения их в новых сферах профессиональной деятельности. *Выпускник умеет:* на достаточном уровне анализировать состояние научно-технической проблемы в профессиональной области деятельности и на этой основе определить цель исследования, методы и средства ее реализации; выбирать и создавать критерии оценки исследований; пользоваться средствами защиты, предоставляемыми ОС; структурировать научное знание, применять современные методы исследований, оценивать и представлять их результаты, аргументировано их защищать; структурировать научное знание, применять современные методы исследований, оценивать и представлять их результаты, аргументировано их защищать; осваивать и использовать новые	4

			методы исследования и применять их в новых сферах профессиональной деятельности. *Выпускник владеет:* на достаточном уровне приёмами прогнозирования тенденций развития науки и техники в профессиональной области деятельности; навыками выбора и создания критериев оценки исследований; навыками администрирования операционных систем; опытом выполнения исследований современными методами в области оптической техники, оптико-электронных приборов и систем, навыками обработки, анализа научных результатов и их представления в наглядном виде; способностью к самостоятельному освоению и использованию новых методов исследования и применения их в новых сферах профессиональной деятельности с достаточной адаптивностью практического навыка.	
		ПОРОГОВЫЙ	*Выпускник знает:* на допустимом уровне основные научные направления развития науки и техники в профессиональной области деятельности; критерии оценки эффективности и надежности средств защиты ОС; основы методологии науки, научные парадигмы, методы научных исследований в смежных областях; эффективные способы освоения и использования новых методов исследования и применения их в новых сферах профессиональной деятельности. *Выпускник умеет:* на допустимом уровне анализировать состояние научно-технической проблемы в профессиональной области деятельности и на этой основе определить цель исследования, методы и средства ее реализации; выбирать и создавать критерии оценки исследований; пользоваться средствами защиты, предоставляемыми ОС; структурировать научное знание, применять современные методы исследований, оценивать и представлять их результаты, аргументировано их защищать; структурировать научное знание, применять современные методы исследований, оценивать и представлять их результаты, аргументировано их защищать; осваивать и использовать новые методы исследования и применять их в новых сферах профессиональной деятельности.	3

			Выпускник владеет: приёмами прогнозирования тенденций развития науки и техники в профессиональной области деятельности; навыками выбора и создания критериев оценки исследований; навыками администрирования операционных систем; опытом выполнения исследований современными методами в области оптической техники, оптико-электронных приборов и систем, навыками обработки, анализа научных результатов и их представления в наглядном виде; способностью к самостоятельному освоению и использованию новых методов исследования и применения их в новых сферах профессиональной деятельности с допустимой адаптивностью практического навыка.	
ПК-1	Способностью анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты	ПОВЫШЕННЫЙ	*Выпускник знает:* на высоком уровне методы и регламенты аудита информационной безопасности информационных систем и объектов информатизации; современные тенденции развития электроники и вычислительной техники, информационных технологий и средств защиты информации; направления развития информационных (телекоммуникационных) технологий; структуру научного познания, его методы и формы, необходимые для анализа направлений развития информационных (телекоммуникационных) технологий; методы прогнозирования эффективности функционирования, оценки затрат и рисков, формирования политики безопасности объектов защиты с учетом специфики этих объектов; жизненный цикл рисковых ситуаций, анализа рисков ИБ, принципы и методы управления рисками информационной безопасности. *Выпускник умеет:* на высоком уровне проводить аудит информационной безопасности информационных систем и объектов информатизации; использовать достижения современных информационных технологий и вычислительной техники для решения профессиональных задач обеспечения безопасности объектов защиты; анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов за-	5

			щиты; прогнозировать эффективность функционирования информационных технологий, оценивать затраты и риски в сфере информационной безопасности с учетом специфики этих объектов; оценивать затраты и риски в сфере информационной безопасности с учетом специфики этих объектов; определять жизненный цикл рисковых ситуаций, анализировать различные риски ИБ, управлять рисками информационной безопасности. *Выпускник владеет:* на высоком уровне навыками и опытом аудита информационной безопасности информационных систем и объектов информатизации; навыком и опытом оценки затрат и рисков при использовании информационных технологий, формирования политики безопасности объектов защиты учетом специфики этих объектов; навыками решения задач прогнозирования эффективности функционирования, оценки затрат и рисков, формирования политики безопасности объектов защиты; навыком формирования политики безопасности объектов защиты учетом специфики этих объектов; навыком и опытом оценки затрат и рисков при использовании информационных технологий; навыком и опытом оценки затрат и рисков при использовании информационных технологий, формирования политики безопасности объектов защиты учетом специфики этих объектов; навыком и опытом определения особенностей жизненного цикла рисковых ситуаций, методикой анализа различных рисков ИБ, возможностями управления рисками информационной безопасности.	
		БАЗОВЫЙ	*Выпускник знает:* на достаточном уровне методы и регламенты аудита информационной безопасности информационных систем и объектов информатизации; современные тенденции развития электроники и вычислительной техники, информационных технологий и средств защиты информации; направления развития информационных (телекоммуникационных) технологий; структуру научного познания, его методы и формы, необходимые для анализа направлений развития информационных (телекоммуникационных) технологий; методы прогнозирования эффективности функционирования,	4

			оценки затрат и рисков, формирования политики безопасности объектов защиты с учетом специфики этих объектов; жизненный цикл рисковых ситуаций, анализа рисков ИБ, принципы и методы управления рисками информационной безопасности. *Выпускник умеет:* на достаточном уровне проводить аудит информационной безопасности информационных систем и объектов информатизации; использовать достижения современных информационных технологий и вычислительной техники для решения профессиональных задач обеспечения безопасности объектов защиты; анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты; прогнозировать эффективность функционирования информационных технологий, оценивать затраты и риски в сфере информационной безопасности с учетом специфики этих объектов; оценивать затраты и риски в сфере информационной безопасности с учетом специфики этих объектов; определять жизненный цикл рисковых ситуаций, анализировать различные риски ИБ, управлять рисками информационной безопасности. *Выпускник владеет:* на достаточном уровне навыками и опытом аудита информационной безопасности информационных систем и объектов информатизации; навыком и опытом оценки затрат и рисков при использовании информационных технологий, формирования политики безопасности объектов защиты учетом специфики этих объектов; навыками решения задач прогнозирования эффективности функционирования, оценки затрат и рисков, формирования политики безопасности объектов защиты; навыком формирования политики безопасности объектов защиты учетом специфики этих объектов; навыком и опытом оценки затрат и рисков при использовании информационных технологий; навыком и опытом оценки затрат и рисков при использовании информационных технологий, формирования политики безопасности объек-	

			тов защиты учетом специфики этих объектов; навыком и опытом определения особенностей жизненного цикла рисковых ситуаций, методикой анализа различных рисков ИБ, возможностями управления рисками информационной безопасности.	
		ПОРОГОВЫЙ	*Выпускник знает:* на допустимом уровне методы и регламенты аудита информационной безопасности информационных систем и объектов информатизации; современные тенденции развития электроники и вычислительной техники, информационных технологий и средств защиты информации; направления развития информационных (телекоммуникационных) технологий; структуру научного познания, его методы и формы, необходимые для анализа направлений развития информационных (телекоммуникационных) технологий; методы прогнозирования эффективности функционирования, оценки затрат и рисков, формирования политики безопасности объектов защиты с учетом специфики этих объектов; жизненный цикл рисковых ситуаций, анализа рисков ИБ, принципы и методы управления рисками информационной безопасности. *Выпускник умеет:* на допустимом уровне проводить аудит информационной безопасности информационных систем и объектов информатизации; использовать достижения современных информационных технологий и вычислительной техники для решения профессиональных задач обеспечения безопасности объектов защиты; анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты; прогнозировать эффективность функционирования информационных технологий, оценивать затраты и риски в сфере информационной безопасности с учетом специфики этих объектов; оценивать затраты и риски в сфере информационной безопасности с учетом специфики этих объектов; определять жизненный цикл рисковых ситуаций, анализировать различные риски ИБ, управлять рисками информационной безопасности.	3

			Выпускник владеет: на допустимом уровне навыками и опытом аудита информационной безопасности информационных систем и объектов информатизации; навыком и опытом оценки затрат и рисков при использовании информационных технологий, формирования политики безопасности объектов защиты учетом специфики этих объектов; навыками решения задач прогнозирования эффективности функционирования, оценки затрат и рисков, формирования политики безопасности объектов защиты; навыком формирования политики безопасности объектов защиты учетом специфики этих объектов; навыком и опытом оценки затрат и рисков при использовании информационных технологий; навыком и опытом оценки затрат и рисков при использовании информационных технологий, формирования политики безопасности объектов защиты учетом специфики этих объектов; навыком и опытом определения особенностей жизненного цикла рисковых ситуаций, методикой анализа различных рисков ИБ, возможностями управления рисками информационной безопасности.	
ПК-2	Способностью разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности	ПОВЫШЕННЫЙ	*Выпускник знает:* на высоком уровне методы и технологии контроля защищенности информации от утечки по техническим каналам и от несанкционированного доступа; общенаучные и специальные методы исследования для выполнения магистерской диссертации; методологию проектирования систем, комплексов, средств и технологий обеспечения информационной безопасности; необходимые для разработки систем, комплексов, средств и технологий обеспечения информационной безопасности нормативно-правовые документы; технические каналы утечки информации; возможности технических разведок; способы и методы научного исследования в профессиональной сфере; системы, комплексы, средства и технологии обеспечения информационной безопасности. *Выпускник умеет:* на высоком уровне разрабатывать системы для контроля защищенности информации от утечки и от несанкционированного доступа; проводить общенаучные и специальные исследования для выполнения ма-	5

			гистерской диссертации; выполнять проектирование и разработку систем, комплексов, средств и технологий обеспечения информационной безопасности; разрабатывать планы защиты объекта с учетом условий эксплуатации; применять на практике методы анализа риска информационной безопасности; использовать новые подходы к организации научно-исследовательской работы в рамках научно-производственного профиля; разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности; *Выпускник владеет:* на высоком уровне навыками применения специальных технических средств для защиты информации от утечки по техническим каналам и от несанкционированного доступа; навыками использования в практической деятельности новых знаний и умений; навыками работы в среде CASE-средств анализа и проектирования систем; методами технической защиты информации; методами формирования требований по защите информации; навыками самостоятельного поиска актуальных направлений научно-исследовательской работы в рамках научного профиля; навыком и опытом разработки систем, комплексов, средств и технологий обеспечения информационной безопасности системы защиты информации техническими средствами.	
		БАЗОВЫЙ	*Выпускник знает:* на достаточном уровне методы и технологии контроля защищенности информации от утечки по техническим каналам и от несанкционированного доступа; общенаучные и специальные методы исследования для выполнения магистерской диссертации; методологию проектирования систем, комплексов, средств и технологий обеспечения информационной безопасности; необходимые для разработки систем, комплексов, средств и технологий обеспечения информационной безопасности нормативно-правовые документы; технические каналы утечки информации; возможности технических разведок; способы и методы научного исследования в профессиональной сфере; системы, комплексы, средства и технологии обеспечения информационной безопасности.	4

			Выпускник умеет: на достаточном уровне разрабатывать системы для контроля защищенности информации от утечки и от несанкционированного доступа; проводить общенаучные и специальные исследования для выполнения магистерской диссертации; выполнять проектирование и разработку систем, комплексов, средств и технологий обеспечения информационной безопасности; разрабатывать планы защиты объекта с учетом условий эксплуатации; применять на практике методы анализа риска информационной безопасности; использовать новые подходы к организации научно-исследовательской работы в рамках научно-производственного профиля; разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности; *Выпускник владеет:* на достаточном уровне навыками применения специальных технических средств для защиты информации от утечки по техническим каналам и от несанкционированного доступа; навыками использования в практической деятельности новых знаний и умений; навыками работы в среде CASE-средств анализа и проектирования систем; методами технической защиты информации; методами формирования требований по защите информации; навыками самостоятельного поиска актуальных направлений научно-исследовательской работы в рамках научного профиля; навыком и опытом разработки систем, комплексов, средств и технологий обеспечения информационной безопасности системы защиты информации техническими средствами.	
		ПОРОГОВЫЙ	*Выпускник знает:* на допустимом уровне методы и технологии контроля защищенности информации от утечки по техническим каналам и от несанкционированного доступа; общенаучные и специальные методы исследования для выполнения магистерской диссертации; методологию проектирования систем, комплексов, средств и технологий обеспечения информационной безопасности; необходимые для разработки систем, комплексов, средств и технологий обеспечения информационной безопасности нормативно-правовые документы; технические	3

			каналы утечки информации; возможности технических разведок; способы и методы научного исследования в профессиональной сфере; системы, комплексы, средства и технологии обеспечения информационной безопасности. *Выпускник умеет:* на допустимом уровне разрабатывать системы для контроля защищенности информации от утечки и от несанкционированного доступа; проводить общенаучные и специальные исследования для выполнения магистерской диссертации; выполнять проектирование и разработку систем, комплексов, средств и технологий обеспечения информационной безопасности; разрабатывать планы защиты объекта с учетом условий эксплуатации; применять на практике методы анализа риска информационной безопасности; использовать новые подходы к организации научно-исследовательской работы в рамках научно-производственного профиля; разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности; *Выпускник владеет:* на допустимом уровне навыками применения специальных технических средств для защиты информации от утечки по техническим каналам и от несанкционированного доступа; навыками использования в практической деятельности новых знаний и умений; навыками работы в среде CASE-средств анализа и проектирования систем; методами технической защиты информации; методами формирования требований по защите информации; навыками самостоятельного поиска актуальных направлений научно-исследовательской работы в рамках научного профиля; навыком и опытом разработки систем, комплексов, средств и технологий обеспечения информационной безопасности системы защиты информации техническими средствами.	
ПК-3	Способностью проводить обоснование состава, характеристик и функциональных возможностей систем и	ПОВЫШЕННЫЙ	*Выпускник знает:* на высоком уровне российские и международные стандарты в области информационной безопасности; основные вопросы современной теории подготовки нормативных документов; состав, характеристики и функциональные возможности систем и средств обеспечения информационной	5

	средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов		безопасности; российские и международные стандарты в сфере информационной безопасности; нормативно-правовые документы в области информационной безопасности, используемые для определения характеристик и функциональных возможностей систем. *Выпускник умеет:* на высоком уровне проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты; применять отечественные и зарубежные стандарты по обеспечению информационной безопасности; разрабатывать и внедрять новейшие информационные технологии; проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов; проводить анализ основных характеристик систем и средств обеспечения информационной безопасности *Выпускник владеет:* на высоком уровне навыками обеспечения информационной безопасности объектов защиты; методикой формирования комплексных мер по защите информации на основе современного законодательства и международных актов и стандартов; навыком и опытом обоснования состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов; навыками обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов.	
		БАЗОВЫЙ	*Выпускник знает:* на достаточном уровне российские и международные стандарты в области информационной безопасности; основные вопросы современной теории подготовки нормативных документов; состав, характеристики и функциональные возможности систем и средств обеспечения информационной безопасности; российские и международные стандарты в сфере информационной безопасности; нормативно-правовые документы в области информационной без-	4

			опасности, используемые для определения характеристик и функциональных возможностей систем. *Выпускник умеет:* на достаточном уровне проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты; применять отечественные и зарубежные стандарты по обеспечению информационной безопасности; разрабатывать и внедрять новейшие информационные технологии; проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов; проводить анализ основных характеристик систем и средств обеспечения информационной безопасности *Выпускник владеет:* на достаточном уровне навыками обеспечения информационной безопасности объектов защиты; методикой формирования комплексных мер по защите информации на основе современного законодательства и международных актов и стандартов; навыком и опытом обоснования состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов; навыками обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов.	
		ПОРОГОВЫЙ	*Выпускник знает:* на допустимом уровне российские и международные стандарты в области информационной безопасности; основные вопросы современной теории подготовки нормативных документов; состав, характеристики и функциональные возможности систем и средств обеспечения информационной безопасности; российские и международные стандарты в сфере информационной безопасности; нормативно-правовые документы в области информационной безопасности, используемые для определения характеристик и функциональных возможностей систем. *Выпускник умеет:*	3

			на допустимом уровне проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты; применять отечественные и зарубежные стандарты по обеспечению информационной безопасности; разрабатывать и внедрять новейшие информационные технологии; проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов; проводить анализ основных характеристик систем и средств обеспечения информационной безопасности *Выпускник владеет:* на допустимом уровне навыками обеспечения информационной безопасности объектов защиты; методикой формирования комплексных мер по защите информации на основе современного законодательства и международных актов и стандартов; навыком и опытом обоснования состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов; навыками обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов.	
ПК-4	Способностью разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности	ПОВЫШЕННЫЙ	*Выпускник знает:* на высоком уровне правила лицензирования и сертификации в области защиты информации; типовые формы документов по подготовке и проведению сертификации и аттестации объектов защиты информации; специальные защитные знаки и их классификацию; основные методы и программы испытания средств обеспечения информационной безопасности; правила и стандарты, регламентирующие процесс формирования научно-технических отчетов; основные требования, предъявляемые к оформлению результатов исследований в виде статей и рефератов; современные средства редактирования и печати, используемые для подготовки к опубликованию результатов выполненных исследований; основные направления регулирования документирования профессиональной деятельно-	5

			сти, структуры его нормативно-методической базы, состав и назначение регулирующих его законодательных актов Российской Федерации; методы и способы разработки программ и методик испытаний средств и систем обеспечения информационной безопасности с учетом их специфики; методику проведения испытаний средств и систем обеспечения информационной безопасности. *Выпускник умеет:* на высоком уровне проводить аудит информационной безопасности предприятий, организаций вне зависимости от их формы собственности и сферы деятельности; проводить испытания средств информационной безопасности; формировать научно-технические отчеты по результатам выполненной работы, оформлять результаты исследований в виде статей и рефератов на базе современных средств редактирования и печати; использовать основные термины документационного обеспечения профессиональной деятельности при составлении документов; использовать в профессиональной деятельности программные средства и средства оргтехники (ксерокс, факс, электронная почта и т.д.); разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности с учетом их специфики; организовывать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами. *Выпускник владеет:* на высоком уровне навыками использования нормативной базы РФ, международных, зарубежных стандартов, лучших практик по обеспечению информационной безопасности предприятий, организаций; навыками применения методик и программ испытания средств обеспечения информационной безопасности; навыком подготовки и оформления научно-технического отчета (магистерской диссертации), статей и рефератов на базе современных средств редактирования и печати; методами создания и оформления основных профессиональных и управленческих документов; компьютерными ин-	

			формационными технологиями в делопроизводстве; навыком и опытом разработки программ и методик испытаний средств и систем обеспечения информационной безопасности с учетом их специфики; навыками по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами.	
		БАЗОВЫЙ	*Выпускник знает:* на достаточном уровне правила лицензирования и сертификации в области защиты информации; типовые формы документов по подготовке и проведению сертификации и аттестации объектов защиты информации; специальные защитные знаки и их классификацию; основные методы и программы испытания средств обеспечения информационной безопасности; правила и стандарты, регламентирующие процесс формирования научно-технических отчетов; основные требования, предъявляемые к оформлению результатов исследований в виде статей и рефератов; современные средства редактирования и печати, используемые для подготовки к опубликованию результатов выполненных исследований; основные направления регулирования документирования профессиональной деятельности, структуры его нормативно-методической базы, состав и назначение регулирующих его законодательных актов Российской Федерации; методы и способы разработки программ и методик испытаний средств и систем обеспечения информационной безопасности с учетом их специфики; методику проведения испытаний средств и систем обеспечения информационной безопасности. *Выпускник умеет:* на достаточном уровне проводить аудит информационной безопасности предприятий, организаций вне зависимости от их формы собственности и сферы деятельности; проводить испытания средств информационной безопасности; формировать научно-технические отчеты по результатам выполненной работы, оформлять результаты исследований в виде статей и рефератов на базе современных средств редактирования и печати; использовать ос-	4

			новные термины документационного обеспечения профессиональной деятельности при составлении документов; использовать в профессиональной деятельности программные средства и средства оргтехники (ксерокс, факс, электронная почта и т.д.); разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности с учетом их специфики; организовывать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами. *Выпускник владеет:* на достаточном уровне навыками использования нормативной базы РФ, международных, зарубежных стандартов, лучших практик по обеспечению информационной безопасности предприятий, организаций; навыками применения методик и программ испытания средств обеспечения информационной безопасности; навыком подготовки и оформления научно-технического отчета (магистерской диссертации), статей и рефератов на базе современных средств редактирования и печати; методами создания и оформления основных профессиональных и управленческих документов; компьютерными информационными технологиями в делопроизводстве; навыком и опытом разработки программ и методик испытаний средств и систем обеспечения информационной безопасности с учетом их специфики; навыками по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами.	
		ПОРОГОВЫЙ	*Выпускник знает:* на допустимом уровне правила лицензирования и сертификации в области защиты информации; типовые формы документов по подготовке и проведению сертификации и аттестации объектов защиты информации; специальные защитные знаки и их классификацию; основные методы и программы испытания средств обеспечения информационной безопасности; правила и	3

			стандарты, регламентирующие процесс формирования научно-технических отчетов; основные требования, предъявляемые к оформлению результатов исследований в виде статей и рефератов; современные средства редактирования и печати, используемые для подготовки к опубликованию результатов выполненных исследований; основные направления регулирования документирования профессиональной деятельности, структуры его нормативно-методической базы, состав и назначение регулирующих его законодательных актов Российской Федерации; методы и способы разработки программ и методик испытаний средств и систем обеспечения информационной безопасности с учетом их специфики; методику проведения испытаний средств и систем обеспечения информационной безопасности. *Выпускник умеет:* на допустимом уровне проводить аудит информационной безопасности предприятий, организаций вне зависимости от их формы собственности и сферы деятельности; проводить испытания средств информационной безопасности; формировать научно-технические отчеты по результатам выполненной работы, оформлять результаты исследований в виде статей и рефератов на базе современных средств редактирования и печати; использовать основные термины документационного обеспечения профессиональной деятельности при составлении документов; использовать в профессиональной деятельности программные средства и средства оргтехники (ксерокс, факс, электронная почта и т.д.); разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности с учетом их специфики; организовывать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами. *Выпускник владеет:* на допустимом уровне навыками использования нормативной базы РФ, международных, зарубежных стандартов, лучших практик по обеспечению информационной	

			безопасности предприятий, организаций; навыками применения методик и программ испытания средств обеспечения информационной безопасности; навыком подготовки и оформления научно-технического отчета (магистерской диссертации), статей и рефератов на базе современных средств редактирования и печати; методами создания и оформления основных профессиональных и управленческих документов; компьютерными информационными технологиями в делопроизводстве; навыком и опытом разработки программ и методик испытаний средств и систем обеспечения информационной безопасности с учетом их специфики; навыками по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами.	
ПК- 5	Способностью анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества	ПОВЫШЕННЫЙ	*Выпускник знает:* на высоком уровне методы критического анализа и оценки современных научных достижений, а также методы генерирования новых идей при решении исследовательских и практических задач в области информационной безопасности; основные научные направления развития науки и техники в профессиональной области деятельности; методы выбора и создания критериев оценки исследований; основные фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества; нормативно-правовые документы по обеспечению информационной безопасности в нашей стране и за рубежом; стандарты построения систем информационной безопасности и стандарты оценки степени защиты систем информационной безопасности объектов; методики анализа рисков информационных систем; методы принятия управленческих решений в системе менеджмента информационной безопасности в условиях риска и неопределённости. *Выпускник умеет:* на высоком уровне уверенно использовать экспериментальные и теоретические методы исследования в предметной сфере профессиональной деятельности; анализи-	5

			ровать состояние научно-технической проблемы в профессиональной области деятельности и на этой основе определить цель исследования, методы и средства ее реализации; выбирать и создавать критерии оценки исследований интерпретировать и обобщать данные, формулировать выводы и рекомендации; применять на практике методы обработки данных; разрабатывать и реализовывать решения, направленные на поддержку социально-значимых проектов и развитие компьютерного творчества; применять методы решения задач информационной безопасности в условиях становления современного информационного общества; выявлять различные сценарии развития рисковых ситуаций в информационном пространстве. *Выпускник владеет:* на высоком уровне навыками критического анализа и оценки современных научных достижений и результатов деятельности по решению исследовательских и практических задач в области информационной безопасности; приёмами прогнозирования тенденций развития науки и техники в профессиональной области деятельности; навыками выбора и создания критериев оценки исследований; навыками решения задач информационной безопасности в условиях становления современного информационного общества; навыками интерпретации и обобщения результатов, формулирования рекомендаций и принятия решений; методологией и навыками решения научных и практических задач; критериями принятия управленческих решений в области информационной безопасности СЭД; навыками выбора оптимального решения при многокритериальных постановках задач.	
		БАЗОВЫЙ	*Выпускник знает:* на достаточном уровне методы критического анализа и оценки современных научных достижений, а также методы генерирования новых идей при решении исследовательских и практических задач в области информационной безопасности; основные научные направления развития науки и техники в профессиональной области деятельности; методы выбора и создания критериев оценки исследований;	4

			основные фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества; нормативно-правовые документы по обеспечению информационной безопасности в нашей стране и за рубежом; стандарты построения систем информационной безопасности и стандарты оценки степени защиты систем информационной безопасности объектов; методики анализа рисков информационных систем; методы принятия управленческих решений в системе менеджмента информационной безопасности в условиях риска и неопределённости. *Выпускник умеет:* на достаточном уровне использовать экспериментальные и теоретические методы исследования в предметной сфере профессиональной деятельности; анализировать состояние научно-технической проблемы в профессиональной области деятельности и на этой основе определить цель исследования, методы и средства ее реализации; выбирать и создавать критерии оценки исследований интерпретировать и обобщать данные, формулировать выводы и рекомендации; применять на практике методы обработки данных; разрабатывать и реализовывать решения, направленные на поддержку социально-значимых проектов и развитие компьютерного творчества; применять методы решения задач информационной безопасности в условиях становления современного информационного общества; выявлять различные сценарии развития рисковых ситуаций в информационном пространстве**.** *Выпускник владеет:* на достаточном уровне навыками критического анализа и оценки современных научных достижений и результатов деятельности по решению исследовательских и практических задач в области информационной безопасности; приёмами прогнозирования тенденций развития науки и техники в профессиональной области деятельности; навыками выбора и создания критериев оценки исследований; навыками решения задач информационной безопасности в условиях становления современного информационного общества; навыками интерпретации и обобщения ре-	

			зультатов, формулирования рекомендаций и принятия решений; методологией и навыками решения научных и практических задач; критериями принятия управленческих решений в области информационной безопасности СЭД; навыками выбора оптимального решения при многокритериальных постановках задач.	
		ПОРОГОВЫЙ	*Выпускник знает:* на допустимом уровне методы критического анализа и оценки современных научных достижений, а также методы генерирования новых идей при решении исследовательских и практических задач в области информационной безопасности; основные научные направления развития науки и техники в профессиональной области деятельности; методы выбора и создания критериев оценки исследований; основные фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества; нормативно-правовые документы по обеспечению информационной безопасности в нашей стране и за рубежом; стандарты построения систем информационной безопасности и стандарты оценки степени защиты систем информационной безопасности объектов; методики анализа рисков информационных систем; методы принятия управленческих решений в системе менеджмента информационной безопасности в условиях риска и неопределённости. *Выпускник умеет:* на допустимом уровне использовать экспериментальные и теоретические методы исследования в предметной сфере профессиональной деятельности; анализировать состояние научно-технической проблемы в профессиональной области деятельности и на этой основе определить цель исследования, методы и средства ее реализации; выбирать и создавать критерии оценки исследований интерпретировать и обобщать данные, формулировать выводы и рекомендации; применять на практике методы обработки данных; разрабатывать и реализовывать решения, направленные на поддержку социально-значимых проектов и развитие компьютерного творчества; применять методы решения задач информационной безопасности в условиях станов-	3

			ления современного информационного общества; выявлять различные сценарии развития рисковых ситуаций в информационном пространстве. *Выпускник владеет:* на допустимом уровне навыками критического анализа и оценки современных научных достижений и результатов деятельности по решению исследовательских и практических задач в области информационной безопасности; приёмами прогнозирования тенденций развития науки и техники в профессиональной области деятельности; навыками выбора и создания критериев оценки исследований; навыками решения задач информационной безопасности в условиях становления современного информационного общества; навыками интерпретации и обобщения результатов, формулирования рекомендаций и принятия решений; методологией и навыками решения научных и практических задач; критериями принятия управленческих решений в области информационной безопасности СЭД; навыками выбора оптимального решения при многокритериальных постановках задач.	
ПК-6	Способностью осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методов и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок	ПОВЫШЕННЫЙ	*Выпускник знает:* на высоком уровне способы сбора, обработки и анализа научно-технической информации по теме исследования; способы анализа имеющейся информации, методологию, конкретные методы и приемы научно - исследовательской деятельности с использованием современных компьютерных технологий; основы методологии научного исследования в области информационной безопасности; принципы проведения библиографической работы с применением современных информационных технологий; Государственные стандарты РФ в области испытания систем и средств ЗИ; требования и стандарты по оценке защищенности СЗИ от НДВ и НСД и их теоретические основы; методы сбора и обработки организационно-распорядительной документации в сфере защиты информации; методику проведения сбора, анализа научно- технической информации, отечественного и зарубежного опыта по тематике исследования; программы проведения научных исследований и технических разработок; методы сбора,	5

			обработки, анализа и систематизации научно-технической информации по теме исследования; российские и международные стандарты в области комплексной безопасности; методы бенчмаркинга и особенности их использования в области информационной безопасности субъектов экономической деятельности; основные подходы к определению экономического ущерба, наносимого информации и информационной системе при реализации угроз информационной безопасности; технологию аналитических исследований информационного пространства субъектов экономической деятельности. *Выпускник умеет:* на высоком уровне выбирать методы и средства решения задачи; систематизировать научно-техническую информацию по теме исследования; выбирать и применять в профессиональной деятельности экспериментальные и расчетно-теоретические методы исследования; формулировать цели, задачи и план научного исследования в области информационной безопасности на основе проведения библиографической работы с применением современных информационных технологий; анализировать и применять стандарты по оценке эффективности систем защиты АС; проводить испытания средств и систем ЗИ; разрабатывать и обрабатывать организационно-распорядительную документацию в сфере защиты информации на основе анализа и систематизации научно-технической информации; проводить сбор, анализ научно-технической информации, отечественного и зарубежного опыта по тематике исследования; осуществлять сбор, обработку, анализ и систематизацию научно-технической информации для защиты информационного пространства; разрабатывать планы и программы проведения научных исследований и технических разработок; проводить обследование текущего уровня обеспечения (уровня зрелости) комплексной безопасности в субъекте экономической деятельности методами бенчмаркинга; организовывать проведение экспериментальных исследований защищенности с применением методов бенчмаркинга; использовать методы экономики при определении эффективности вложений в систему ком-	

			плексной безопасности в организации; использовать методы экономики при определении эффективности вложений в систему комплексной безопасности в организации *Выпускник владеет:* на высоком уровне навыками разработок планов и программ проведения научных исследований и технических разработок; навыками планирования научного исследования, анализа получаемых результатов и формулировки выводов; опытом разработки технического задания на проведение научно-исследовательской работы в области информационной безопасности, в том числе ее целей, задач и плана; навыком библиографического поиска по заданной теме с применением современных информационных технологий; представлением о методах оценки эффективности систем и средств ЗИ; о методах оценки защищенности СЗИ и контроля отсутствия недекларированных и недокументированных возможностей; специальными программными средствами по созданию организационно-распорядительной документации в сфере защиты информации; навыками сбора, анализа научно-технической информации, отечественного и зарубежного опыта по тематике исследования; навыками проведения применения методов бенчмаркинга в области ИБ для совершенствования бизнес процессов, аналитических исследований в области комплексной безопасности; выбора методов и средств решения задач; анализа и систематизации научно-технической информации по теме исследования; выбора методов и средств решения задач обеспечения комплексной безопасности; опытом обеспечивающих комплексную безопасность; методами проведения анализа рисков информационной безопасности объектов оценки с использованием отечественных и международных стандартов и с привлечением современного программного инструментария.	
		БАЗОВЫЙ	*Выпускник знает:* на достаточном уровне способы сбора, обработки и анализа научно-технической информации по теме исследования; способы анализа имеющейся информации, методологию, конкретные методы и приемы научно - исследовательской деятельности с использованием современных компьютер-	4

			ных технологий; основы методологии научного исследования в области информационной безопасности; принципы проведения библиографической работы с применением современных информационных технологий; Государственные стандарты РФ в области испытания систем и средств ЗИ; требования и стандарты по оценке защищенности СЗИ от НДВ и НСД и их теоретические основы; методы сбора и обработки организационно-распорядительной документации в сфере защиты информации; методику проведения сбора, анализа научно- технической информации, отечественного и зарубежного опыта по тематике исследования; программы проведения научных исследований и технических разработок; методы сбора, обработки, анализа и систематизации научно-технической информации по теме исследования; российские и международные стандарты в области комплексной безопасности; методы бенчмаркинга и особенности их использования в области информационной безопасности субъектов экономической деятельности; основные подходы к определению экономического ущерба, наносимого информации и информационной системе при реализации угроз информационной безопасности; технологию аналитических исследований информационного пространства субъектов экономической деятельности. *Выпускник умеет:* на достаточном уровне выбирать методы и средства решения задачи; систематизировать научно-техническую информацию по теме исследования; выбирать и применять в профессиональной деятельности экспериментальные и расчетно-теоретические методы исследования; формулировать цели, задачи и план научного исследования в области информационной безопасности на основе проведения библиографической работы с применением современных информационных технологий; анализировать и применять стандарты по оценке эффективности систем защиты АС; проводить испытания средств и систем ЗИ; разрабатывать и обрабатывать организационно-распорядительную документацию в сфере защиты информации на основе анализа и систематизации научно-	

			технической информации; проводить сбор, анализ научно-технической информации, отечественного и зарубежного опыта по тематике исследования; осуществлять сбор, обработку, анализ и систематизацию научно-технической информации для защиты информационного пространства; разрабатывать планы и программы проведения научных исследований и технических разработок; проводить обследование текущего уровня обеспечения (уровня зрелости) комплексной безопасности в субъекте экономической деятельности методами бенчмаркинга; организовывать проведение экспериментальных исследований защищенности с применением методов бенчмаркинга; использовать методы экономики при определении эффективности вложений в систему комплексной безопасности в организации; использовать методы экономики при определении эффективности вложений в систему комплексной безопасности в организации *Выпускник владеет:* на достаточном уровне навыками разработок планов и программ проведения научных исследований и технических разработок; навыками планирования научного исследования, анализа получаемых результатов и формулировки выводов; опытом разработки технического задания на проведение научно-исследовательской работы в области информационной безопасности, в том числе ее целей, задач и плана; навыком библиографического поиска по заданной теме с применением современных информационных технологий; представлением о методах оценки эффективности систем и средств ЗИ; о методах оценки защищенности СЗИ и контроля отсутствия недекларированных и недокументированных возможностей; специальными программными средствами по созданию организационно-распорядительной документации в сфере защиты информации; навыками сбора, анализа научно-технической информации, отечественного и зарубежного опыта по тематике исследования; навыками проведения применения методов бенчмаркинга в области ИБ для совершенствования бизнес процессов, аналитических исследований в области комплексной безопасности; выбора методов и средств	

			решения задач; анализа и систематизации научно-технической информации по теме исследования; выбора методов и средств решения задач обеспечения комплексной безопасности; опытом обеспечивающих комплексную безопасность; методами проведения анализа рисков информационной безопасности объектов оценки с использованием отечественных и международных стандартов и с привлечением современного программного инструментария.	
		ПОРОГОВЫЙ	*Выпускник знает:* на допустимом уровне способы сбора, обработки и анализа научно-технической информации по теме исследования; способы анализа имеющейся информации, методологию, конкретные методы и приемы научно - исследовательской деятельности с использованием современных компьютерных технологий; основы методологии научного исследования в области информационной безопасности; принципы проведения библиографической работы с применением современных информационных технологий; Государственные стандарты РФ в области испытания систем и средств ЗИ; требования и стандарты по оценке защищенности СЗИ от НДВ и НСД и их теоретические основы; методы сбора и обработки организационно-распорядительной документации в сфере защиты информации; методику проведения сбора, анализа научно- технической информации, отечественного и зарубежного опыта по тематике исследования; программы проведения научных исследований и технических разработок; методы сбора, обработки, анализа и систематизации научно-технической информации по теме исследования; российские и международные стандарты в области комплексной безопасности; методы бенчмаркинга и особенности их использования в области информационной безопасности субъектов экономической деятельности; основные подходы к определению экономического ущерба, наносимого информации и информационной системе при реализации угроз информационной безопасности; технологию аналитических исследований информационного пространства субъектов экономической деятельности.	З

			Выпускник умеет: на допустимом уровне выбирать методы и средства решения задачи; систематизировать научно-техническую информацию по теме исследования; выбирать и применять в профессиональной деятельности экспериментальные и расчетно-теоретические методы исследования; формулировать цели, задачи и план научного исследования в области информационной безопасности на основе проведения библиографической работы с применением современных информационных технологий; анализировать и применять стандарты по оценке эффективности систем защиты АС; проводить испытания средств и систем ЗИ; разрабатывать и обрабатывать организационно-распорядительную документацию в сфере защиты информации на основе анализа и систематизации научно-технической информации; проводить сбор, анализ научно-технической информации, отечественного и зарубежного опыта по тематике исследования; осуществлять сбор, обработку, анализ и систематизацию научно-технической информации для защиты информационного пространства; разрабатывать планы и программы проведения научных исследований и технических разработок; проводить обследование текущего уровня обеспечения (уровня зрелости) комплексной безопасности в субъекте экономической деятельности методами бенчмаркинга; организовывать проведение экспериментальных исследований защищенности с применением методов бенчмаркинга; использовать методы экономики при определении эффективности вложений в систему комплексной безопасности в организации; использовать методы экономики при определении эффективности вложений в систему комплексной безопасности в организации *Выпускник владеет:* на допустимом уровне навыками разработок планов и программ проведения научных исследований и технических разработок; навыками планирования научного исследования, анализа получаемых результатов и формулировки выводов; опытом разработки технического задания на проведение научно-исследовательской работы в области информационной безопасности, в том числе ее целей, задач и плана; навы-	

			ком библиографического поиска по заданной теме с применением современных информационных технологий; представлением о методах оценки эффективности систем и средств ЗИ; о методах оценки защищенности СЗИ и контроля отсутствия недекларированных и недокументированных возможностей; специальными программными средствами по созданию организационно-распорядительной документации в сфере защиты информации; навыками сбора, анализа научно-технической информации, отечественного и зарубежного опыта по тематике исследования; навыками проведения применения методов бенчмаркинга в области ИБ для совершенствования бизнес процессов, аналитических исследований в области комплексной безопасности; выбора методов и средств решения задач; анализа и систематизации научно-технической информации по теме исследования; выбора методов и средств решения задач обеспечения комплексной безопасности; опытом обеспечивающих комплексную безопасность; методами проведения анализа рисков информационной безопасности объектов оценки с использованием отечественных и международных стандартов и с привлечением современного программного инструментария.	
ПК-7	Способностью проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента	ПОВЫШЕННЫЙ	*Выпускник знает:* на высоком уровне физические и математические методы исследования защищенности объектов; методы экспериментальных исследований для цифровой обработки изображений; методы экспериментальных исследований для выявления несанкционированного доступа и технических каналов утечки информации; основные принципы проектирования современных сетей связи**,** основные термины и определения предметной области «маршрутизация» в сетях связи, методы организации защищённых сетей с применением специальных технических и программных методов; основные виды математических моделей объектов исследования, основные алгоритмы решения задач; основные экспериментальные методики и технические средства измерения физических величин; методы поддержки организационно-управленческих решений в системе ме-	5

			неджмента информационной безопасности; современные экономические подходы и методы определения экономической эффективности системы защиты информации субъекта экономической деятельности. *Выпускник умеет:* на высоком уровне проводить экспериментальные исследования защищенности объектов; проводить исследования по выявлению каналов несанкционированного доступа и утечки информации; проектировать сети связи, в части транспортного сегмента, а так же сети абонентского доступа с применением соответствующих физических и математических методов; точно и грамотно строить математические модели, независимо от их степени сложности; проводить экспериментальные исследования защищенности объектов; применять современные информационные технологии, поддерживающие организационно-управленческие решения в системе менеджмента информационной безопасности; проводить анализ рисков информационной безопасности объектов и систем с использованием отечественных и международных стандартов; применять физические и математические методы, технические и программные средства цифровой обработки изображений. *Выпускник владеет:* на высоком уровне навыками применения технических и программных средств обработки результатов эксперимента; средствами обработки результатов исследований по выявлению каналов несанкционированного доступа и утечки информации; основными этапами проектирования телекоммуникационных сетей; опытом построения математических моделей объектов исследования и выбора численных методов их моделирования, навыком создания новых алгоритмов решения задач; навыками применения технических и программных средств обработки результатов эксперимента; принятия организационно-управленческих решений в системе менеджмента информационной безопасности; современными экономическими подходами к расчету эффективности затрат на комплексную систему обеспечения информационной безопасности; программными средствами цифровой обработки	

			изображений.	
		БАЗОВЫЙ	*Выпускник знает:* на достаточном уровне физические и математические методы исследования защищенности объектов; методы экспериментальных исследований для цифровой обработки изображений; методы экспериментальных исследований для выявления несанкционированного доступа и технических каналов утечки информации; основные принципы проектирования современных сетей связи**,** основные термины и определения предметной области «маршрутизация» в сетях связи, методы организации защищённых сетей с применением специальных технических и программных методов; основные виды математических моделей объектов исследования, основные алгоритмы решения задач; основные экспериментальные методики и технические средства измерения физических величин; методы поддержки организационно-управленческих решений в системе менеджмента информационной безопасности; современные экономические подходы и методы определения экономической эффективности системы защиты информации субъекта экономической деятельности. *Выпускник умеет:* на достаточном уровне проводить экспериментальные исследования защищенности объектов; проводить исследования по выявлению каналов несанкционированного доступа и утечки информации; проектировать сети связи, в части транспортного сегмента, а так же сети абонентского доступас применением соответствующих физических и математических методов; точно и грамотно строить математические модели, независимо от их степени сложности; проводить экспериментальные исследования защищенности объектов; применять современные информационные технологии, поддерживающие организационно-управленческие решения в системе менеджмента информационной безопасности; проводить анализ рисков информационной безопасности объектов и систем с использованием отечественных и международных стандартов; применять физические и математические методы, технические и программные средства цифровой обработки изображений.	4

			Выпускник владеет: на достаточном уровне навыками применения технических и программных средств обработки результатов эксперимента; средствами обработки результатов исследований по выявлению каналов несанкционированного доступа и утечки информации; основными этапами проектирования телекоммуникационных сетей; опытом построения математических моделей объектов исследования и выбора численных методов их моделирования, навыком создания новых алгоритмов решения задач; навыками применения технических и программных средств обработки результатов эксперимента; принятия организационно-управленческих решений в системе менеджмента информационной безопасности; современными экономическими подходами к расчету эффективности затрат на комплексную систему обеспечения информационной безопасности; программными средствами цифровой обработки изображений.	
		ПОРОГОВЫЙ	*Выпускник знает:* на допустимом уровне физические и математические методы исследования защищенности объектов; методы экспериментальных исследований для цифровой обработки изображений; методы экспериментальных исследований для выявления несанкционированного доступа и технических каналов утечки информации; основные принципы проектирования современных сетей связи**,** основные термины и определения предметной области «маршрутизация» в сетях связи, методы организации защищённых сетей с применением специальных технических и программных методов; основные виды математических моделей объектов исследования, основные алгоритмы решения задач; основные экспериментальные методики и технические средства измерения физических величин; методы поддержки организационно-управленческих решений в системе менеджмента информационной безопасности; современные экономические подходы и методы определения экономической эффективности системы защиты информации субъекта экономической деятельности. *Выпускник умеет:* на допустимом уровне проводить экспе-	3

			риментальные исследования защищенности объектов; проводить исследования по выявлению каналов несанкционированного доступа и утечки информации; проектировать сети связи, в части транспортного сегмента, а так же сети абонентского доступас применением соответствующих физических и математических методов; точно и грамотно строить математические модели, независимо от их степени сложности; проводить экспериментальные исследования защищенности объектов; применять современные информационные технологии, поддерживающие организационно-управленческие решения в системе менеджмента информационной безопасности; проводить анализ рисков информационной безопасности объектов и систем с использованием отечественных и международных стандартов; применять физические и математические методы, технические и программные средства цифровой обработки изображений. *Выпускник владеет:* на допустимом уровне навыками применения технических и программных средств обработки результатов эксперимента; средствами обработки результатов исследований по выявлению каналов несанкционированного доступа и утечки информации; основными этапами проектирования телекоммуникационных сетей; опытом построения математических моделей объектов исследования и выбора численных методов их моделирования, навыком создания новых алгоритмов решения задач; навыками применения технических и программных средств обработки результатов эксперимента; принятия организационно-управленческих решений в системе менеджмента информационной безопасности; современными экономическими подходами к расчету эффективности затрат на комплексную систему обеспечения информационной безопасности; программными средствами цифровой обработки изображений.	
ПК-8	Способностью обрабатывать результаты экспериментальных исследований,	ПОВЫШЕННЫЙ	*Выпускник знает:* на высоком уровне об установлении истины, методы научного исследования путём мысленного расчленения объекта (анализ) и путём изучения предмета в его целостности, единстве его частей (синтез); ос-	5

	оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи		новные методы обработки результатов исследования эффективности и защищенности телекоммуникационных систем; алгоритмы разработки и оптимизации программ экспериментальных исследований, статистические методы обработки экспериментальных результатов; правила и стандарты, регламентирующие процесс формирования научно-технических отчетов; основные требования, предъявляемые к оформлению результатов исследований в виде статей и рефератов; современные средства редактирования и печати, используемые для подготовки к опубликованию результатов выполненных исследований; правила и стандарты, регламентирующие процесс формирования научно-технических отчетов; основные требования, предъявляемые к оформлению результатов исследований; основные методы цифровой обработки изображений; процессы и процедуры экспериментальных исследований системы управления информационной безопасностью. *Выпускник умеет:* на высоком уровне использовать методы абстрактного мышления, анализа и синтеза; выявлять альтернативные варианты решения исследовательских задач и оценивать экономическую эффективность реализации этих вариантов; оформлять техническую документацию в сфере защиты телекоммуникационных систем и систем передачи данных; разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности с учетом их специфики; формировать научно-технические отчеты по результатам выполненной работы, оформлять результаты исследований в виде статей и рефератов на базе современных средств редактирования и печати; оформлять научно-технические отчеты, обзоры по предметной области; прогнозировать состояние комплексной безопасности СЭД на основе проведенного анализа и используемых методик бенчмаркинга; оформлять техническую документацию результатов цифровой обработки изображений; разрабатывать предложения по совершенствованию методик исследований систем управления информационной безопасностью. *Выпускник владеет:*	

			на высоком уровне целостной системой навыков использования абстрактного мышления при решении проблем, возникающих при выполнении исследовательских работ, навыками отстаивания своей точки зрения; навыками работы в специальных программных средствах для оформления результатов экспериментальных исследований; навыком и опытом разработки программ и методик испытаний средств и систем обеспечения информационной безопасности с учетом их специфики; навыками подготовки по результатам выполненных исследований научных докладов и статей в области информационной безопасности; навыками стратегического планирования функционирования СЭД в области КБ и решения совокупности задач, связанных с организацией управления информационной безопасностью СЭД ;навыками работы в специальных программных средствах для цифровой обработки изображений; навыками обоснования предложений по совершенствованию методик исследования систем управления информационной безопасностью.	
		БАЗОВЫЙ	*Выпускник знает:* на достаточном уровне об установлении истины, методы научного исследования путём мысленного расчленения объекта (анализ) и путём изучения предмета в его целостности, единстве его частей (синтез); основные методы обработки результатов исследования эффективности и защищенности телекоммуникационных систем; алгоритмы разработки и оптимизации программ экспериментальных исследований, статистические методы обработки экспериментальных результатов; правила и стандарты, регламентирующие процесс формирования научно-технических отчетов; основные требования, предъявляемые к оформлению результатов исследований в виде статей и рефератов; современные средства редактирования и печати, используемые для подготовки к опубликованию результатов выполненных исследований; правила и стандарты, регламентирующие процесс формирования научно-технических отчетов; основные требования, предъявляемые к оформлению результатов исследований; основные методы цифровой обработки изображений	4

			;процессы и процедуры экспериментальных исследований системы управления информационной безопасностью. *Выпускник умеет:* на достаточном уровне использовать методы абстрактного мышления, анализа и синтеза; выявлять альтернативные варианты решения исследовательских задач и оценивать экономическую эффективность реализации этих вариантов; оформлять техническую документацию в сфере защиты телекоммуникационных систем и систем передачи данных; разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности с учетом их специфики; формировать научно-технические отчеты по результатам выполненной работы, оформлять результаты исследований в виде статей и рефератов на базе современных средств редактирования и печати; оформлять научно-технические отчеты, обзоры по предметной области; прогнозировать состояние комплексной безопасности СЭД на основе проведенного анализа и используемых методик бенчмаркинга; оформлять техническую документацию результатов цифровой обработки изображений; разрабатывать предложения по совершенствованию методик исследований систем управления информационной безопасностью. *Выпускник владеет:* на достаточном уровне целостной системой навыков использования абстрактного мышления при решении проблем, возникающих при выполнении исследовательских работ, навыками отстаивания своей точки зрения; навыками работы в специальных программных средствах для оформления результатов экспериментальных исследований; навыком и опытом разработки программ и методик испытаний средств и систем обеспечения информационной безопасности с учетом их специфики; навыками подготовки по результатам выполненных исследований научных докладов и статей в области информационной безопасности; навыками стратегического планирования функционирования СЭД в области КБ и решения совокупности задач, связанных с организацией управления информационной безопасно-	

			стью СЭД; навыками работы в специальных программных средствах для цифровой обработки изображений; навыками обоснования предложений по совершенствованию методик исследования систем управления информационной безопасностью.	
		ПОРОГОВЫЙ	*Выпускник знает:* на допустимом уровне об установлении истины, методы научного исследования путём мысленного расчленения объекта (анализ) и путём изучения предмета в его целостности, единстве его частей (синтез); основные методы обработки результатов исследования эффективности и защищенности телекоммуникационных систем; алгоритмы разработки и оптимизации программ экспериментальных исследований, статистические методы обработки экспериментальных результатов; правила и стандарты, регламентирующие процесс формирования научно-технических отчетов; основные требования, предъявляемые к оформлению результатов исследований в виде статей и рефератов; современные средства редактирования и печати, используемые для подготовки к опубликованию результатов выполненных исследований; правила и стандарты, регламентирующие процесс формирования научно-технических отчетов; основные требования, предъявляемые к оформлению результатов исследований; основные методы цифровой обработки изображений; процессы и процедуры экспериментальных исследований системы управления информационной безопасностью. *Выпускник умеет:* на допустимом уровне использовать методы абстрактного мышления, анализа и синтеза; выявлять альтернативные варианты решения исследовательских задач и оценивать экономическую эффективность реализации этих вариантов ;оформлять техническую документацию в сфере защиты телекоммуникационных систем и систем передачи данных; разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности с учетом их специфики; формировать научно-технические отчеты по результатам выполненной работы, оформлять результаты исследований в виде статей и рефератов на базе современных	3

			средств редактирования и печати; оформлять научно-технические отчеты, обзоры по предметной области; прогнозировать состояние комплексной безопасности СЭД на основе проведенного анализа и используемых методик бенчмаркинга; оформлять техническую документацию результатов цифровой обработки изображений; разрабатывать предложения по совершенствованию методик исследований систем управления информационной безопасностью. *Выпускник владеет:* на допустимом уровне целостной системой навыков использования абстрактного мышления при решении проблем, возникающих при выполнении исследовательских работ, навыками отстаивания своей точки зрения; навыками работы в специальных программных средствах для оформления результатов экспериментальных исследований; навыком и опытом разработки программ и методик испытаний средств и систем обеспечения информационной безопасности с учетом их специфики; навыками подготовки по результатам выполненных исследований научных докладов и статей в области информационной безопасности; навыками стратегического планирования функционирования СЭД в области КБ и решения совокупности задач, связанных с организацией управления информационной безопасностью СЭД; навыками работы в специальных программных средствах для цифровой обработки изображений; навыками обоснования предложений по совершенствованию методик исследования систем управления информационной безопасностью.	
ПК-12	Способностью организовать выполнение работ, управлять коллективом исполнителей и принимать управленческие решения	ПОВЫШЕННЫЙ	*Выпускник знает:* на высоком уровне роль человеческого фактора в успешной реализации проекта; порядок выполнения работ для оценки угроз и рисков информационной безопасности предприятий; основы деятельности в подразделениях аналитического управления; принципы организации работы коллектива в сфере управления информационной безопасностью и этапы жизненного цикла информационных систем; процессы и процедуры планирования системы управления информационной безопасностью.	5

			Выпускник умеет: на высоком уровне выбирать рациональные методы и средства управления проектом; принимать управленческие решения для защиты информационного пространства предприятий; организовать выполнение работ, связанных с мониторингом внешней среды и внутренних показателей; управлять коллективом и принимать управленческие решения с учетом жизненного цикла информационных систем; использовать рискориентированную методологию управления информационной безопасностью. *Выпускник владеет:* на высоком уровне навыками формирования графика хода реализации проекта; навыками управления коллективом исполнителей для решения задач зашиты информационного пространства; навыками управления коллективом соисполнителей; методами организации выполнения работ, учитывая технические, организационные и кадровые аспекты управления информационной безопасностью; навыками определения правил и процедур управления информационной безопасностью; навыками определения правил и процедур управления информационной безопасностью; методами принятия управленческих решений, учитывая с учетом жизненного цикла информационных систем.	
		БАЗОВЫЙ	*Выпускник знает:* на достаточном уровне роль человеческого фактора в успешной реализации проекта; порядок выполнения работ для оценки угроз и рисков информационной безопасности предприятий; основы деятельности в подразделениях аналитического управления; принципы организации работы коллектива в сфере управления информационной безопасностью и этапы жизненного цикла информационных систем; процессы и процедуры планирования системы управления информационной безопасностью. *Выпускник умеет:* на достаточном уровне выбирать рациональные методы и средства управления проектом; принимать управленческие решения для защиты информационного пространства предприятий; организовать выполнение работ, связанных с мониторин-	4

			гом внешней среды и внутренних показателей; управлять коллективом и принимать управленческие решения с учетом жизненного цикла информационных систем; использовать рискориентированную методологию управления информационной безопасностью. *Выпускник владеет:* на достаточном уровне навыками формирования графика хода реализации проекта; навыками управления коллективом исполнителей для решения задач зашиты информационного пространства; навыками управления коллективом соисполнителей; методами организации выполнения работ, учитывая технические, организационные и кадровые аспекты управления информационной безопасностью; навыками определения правил и процедур управления информационной безопасностью; навыками определения правил и процедур управления информационной безопасностью; методами принятия управленческих решений, учитывая с учетом жизненного цикла информационных систем.	
		ПОРОГОВЫЙ	*Выпускник знает:* на допустимом уровне роль человеческого фактора в успешной реализации проекта; порядок выполнения работ для оценки угроз и рисков информационной безопасности предприятий; основы деятельности в подразделениях аналитического управления; принципы организации работы коллектива в сфере управления информационной безопасностью и этапы жизненного цикла информационных систем; процессы и процедуры планирования системы управления информационной безопасностью. *Выпускник умеет:* на допустимом уровне выбирать рациональные методы и средства управления проектом; принимать управленческие решения для защиты информационного пространства предприятий; организовать выполнение работ, связанных с мониторингом внешней среды и внутренних показателей; управлять коллективом и принимать управленческие решения с учетом жизненного цикла информационных систем; использовать рискориентированную методологию управления информационной безопасностью.	3

			Выпускник владеет: на допустимом уровне навыками формирования графика хода реализации проекта; навыками управления коллективом исполнителей для решения задач зашиты информационного пространства; навыками управления коллективом соисполнителей; методами организации выполнения работ, учитывая технические, организационные и кадровые аспекты управления информационной безопасностью; навыками определения правил и процедур управления информационной безопасностью; навыками определения правил и процедур управления информационной безопасностью; методами принятия управленческих решений, учитывая с учетом жизненного цикла информационных систем.	
ПК-13	Способностью организовать управление информационной безопасностью	ПОВЫШЕННЫЙ	*Выпускник знает:* на высоком уровне порядок организации деятельности по управлению информационной безопасностью; порядок выполнения работ для оценки угроз и рисков информационной безопасности предприятия; принципы организации управления информационной безопасностью; основные методы управленческой деятельности, состав системы управления информационной безопасностью и требования к ее элементам; основные методы управления защитой информации; основные направления развития информационных технологий, принципы и методы формирования политики безопасности объектов защиты с учетом специфики этих объектов. *Выпускник умеет:* на высоком уровне организовать процесс управления информационной безопасностью; принимать управленческие решения для защиты информационного пространства предприятия; принимать управленческие решения в сфере управления информационной безопасностью; определять комплекс мер (правила, процедуры, практические приемы, методы, средства) для обеспечения информационной безопасности информационных систем; выбирать меры и средства защиты информации для использования их с целью обеспечения требуемого уровня защищённости; прогнозировать эффективность функционирования информационных технологий, оценивать затраты и риски в сфере информаци-	5

			онной безопасности с учетом специфики этих объектов *Выпускник владеет:* на высоком уровне навыками управления системой информационной безопасности; навыками управления коллективом исполнителей решения задач зашиты информационного пространства; навыками управления коллективом, учитывая технические, организационные и кадровые аспекты управления информационной безопасностью; навыками анализа информационной инфраструктуры предприятия и ее безопасности; методами управления информационной безопасностью информационных систем; навыками обоснования и контроля результатов управленческих решений в области безопасности информации; навыком и опытом оценки затрат и рисков при использовании информационных технологий, формирования политики безопасности объектов защиты учетом специфики этих объектов.	
		БАЗОВЫЙ	*Выпускник знает:* на достаточном уровне порядок организации деятельности по управлению информационной безопасностью; порядок выполнения работ для оценки угроз и рисков информационной безопасности предприятия; принципы организации управления информационной безопасностью; основные методы управленческой деятельности, состав системы управления информационной безопасностью и требования к ее элементам; основные методы управления защитой информации; основные направления развития информационных технологий, принципы и методы формирования политики безопасности объектов защиты с учетом специфики этих объектов. *Выпускник умеет:* на достаточном уровне организовать процесс управления информационной безопасностью; принимать управленческие решения для защиты информационного пространства предприятия; принимать управленческие решения в сфере управления информационной безопасностью; определять комплекс мер (правила, процедуры, практические приемы, методы, средства) для обеспечения информационной безопасности информационных систем; выбирать меры и средства защиты инфор-	4

			мации для использования их с целью обеспечения требуемого уровня защищённости; прогнозировать эффективность функционирования информационных технологий, оценивать затраты и риски в сфере информационной безопасности с учетом специфики этих объектов *Выпускник владеет:* на достаточном уровне навыками управления системой информационной безопасности; навыками управления коллективом исполнителей решения задач зашиты информационного пространства; навыками управления коллективом, учитывая технические, организационные и кадровые аспекты управления информационной безопасностью; навыками анализа информационной инфраструктуры предприятия и ее безопасности; методами управления информационной безопасностью информационных систем; навыками обоснования и контроля результатов управленческих решений в области безопасности информации; навыком и опытом оценки затрат и рисков при использовании информационных технологий, формирования политики безопасности объектов защиты учетом специфики этих объектов.	
		ПОРОГОВЫЙ	*Выпускник знает:* на допустимом уровне порядок организации деятельности по управлению информационной безопасностью; порядок выполнения работ для оценки угроз и рисков информационной безопасности предприятия; принципы организации управления информационной безопасностью; основные методы управленческой деятельности, состав системы управления информационной безопасностью и требования к ее элементам; основные методы управления защитой информации; основные направления развития информационных технологий, принципы и методы формирования политики безопасности объектов защиты с учетом специфики этих объектов. *Выпускник умеет:* на допустимом уровне организовать процесс управления информационной безопасностью; принимать управленческие решения для защиты информационного пространства предприятия; принимать управленческие решения в сфере управления информационной безопасностью;	3

			определять комплекс мер (правила, процедуры, практические приемы, методы, средства) для обеспечения информационной безопасности информационных систем; выбирать меры и средства защиты информации для использования их с целью обеспечения требуемого уровня защищённости; прогнозировать эффективность функционирования информационных технологий, оценивать затраты и риски в сфере информационной безопасности с учетом специфики этих объектов *Выпускник владеет:* на допустимом уровне навыками управления системой информационной безопасности; навыками управления коллективом исполнителей решения задач зашиты информационного пространства; навыками управления коллективом, учитывая технические, организационные и кадровые аспекты управления информационной безопасностью; навыками анализа информационной инфраструктуры предприятия и ее безопасности; методами управления информационной безопасностью информационных систем; навыками обоснования и контроля результатов управленческих решений в области безопасности информации; навыком и опытом оценки затрат и рисков при использовании информационных технологий, формирования политики безопасности объектов защиты учетом специфики этих объектов.	
ПК-14	Способностью организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России	ПОВЫШЕННЫЙ	*Выпускник знает:* на высоком уровне основные понятия и содержание основных нормативных правовых актов в сфере информационной безопасности; основные нормативные акты и нормативные методические документы ФСБ России, ФСТЭК России; стандарты и спецификации в области информационной безопасности. *Выпускник умеет:* на высоком уровне разрабатывать организационные и нормативно-методические материалы в целях обеспечения информационной безопасности; выбирать методы и средства обеспечения информационной безопасности для использования их с целью обеспечения требуемого уровня защищённости; организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной	5

			безопасности; организовать технологический процесс защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю *Выпускник владеет:* на высоком уровне методикой использования компьютерной техники и информационных технологий при составлении и оформлении документации, связанной с международными и Российскими актами и стандартами информационной безопасности; навыками применения нормативно-методической документации при создании или модернизации систем, средств и технологий обеспечения информационной безопасности; методиками организации технологического процесса защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю	
		БАЗОВЫЙ	*Выпускник знает:* на достаточном уровне основные понятия и содержание основных нормативных правовых актов в сфере информационной безопасности; основные нормативные акты и нормативные методические документы ФСБ России, ФСТЭК России; стандарты и спецификации в области информационной безопасности. *Выпускник умеет:* на достаточном уровне разрабатывать организационные и нормативно-методические материалы в целях обеспечения информационной безопасности; выбирать методы и средства обеспечения информационной безопасности для использования их с целью обеспечения требуемого уровня защищённости; организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности; организовать технологический процесс защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации,	4

			Федеральной службой по техническому и экспортному контролю *Выпускник владеет:* на достаточном уровне методикой использования компьютерной техники и информационных технологий при составлении и оформлении документации, связанной с международными и Российскими актами и стандартами информационной безопасности; навыками применения нормативно-методической документации при создании или модернизации систем, средств и технологий обеспечения информационной безопасности; методиками организации технологического процесса защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю	
		ПОРОГОВЫЙ	*Выпускник знает:* на допустимом уровне основные понятия и содержание основных нормативных правовых актов в сфере информационной безопасности; основные нормативные акты и нормативные методические документы ФСБ России, ФСТЭК России; стандарты и спецификации в области информационной безопасности. *Выпускник умеет:* на допустимом уровне разрабатывать организационные и нормативно-методические материалы в целях обеспечения информационной безопасности; выбирать методы и средства обеспечения информационной безопасности для использования их с целью обеспечения требуемого уровня защищённости; организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности; организовать технологический процесс защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю *Выпускник владеет:* на допустимом уровне методикой использования компьютерной техники и информационных технологий при составлении и	3

			оформлении документации, связанной с международными и Российскими актами и стандартами информационной безопасности; навыками применения нормативно-методической документации при создании или модернизации систем, средств и технологий обеспечения информационной безопасности; методиками организации технологического процесса защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю	
ПК-15	Способностью организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности	ПОВЫШЕННЫЙ	*Выпускник знает:* на высоком уровне порядок проведения аттестации объектов информационной защиты; типовые методики испытаний объектов информатизации по требованиям защиты информации; системы и средства обеспечения информационной безопасности, необходимые для организации выполнения работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности сведения; методологию создания систем защиты информации; перспективные направления развития средств и методов защиты информации; основные положения существующей законодательной базы и нормативные документы в области информационной безопасности; методы аттестации уровня защищенности информационных систем. *Выпускник умеет:* на высоком уровне определять угрозы объекту информатизации; определять рациональные способы и средства защиты информации на объекте информатизации; организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности; организовать технологический процесс защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю; определять комплекс мер для обеспечения ввода в эксплуатацию систем информационной безопасности. *Выпускник владеет:*	5

			на высоком уровне навыками и опытом организации мероприятий по защите информации на объекте информатизации; навыками введения в эксплуатацию систем и средств обеспечения информационной безопасности; навыками работы с нормативными документами; правилами составления локальных нормативных актов и регламентов в области информационной безопасности; навыками подготовки отчетных и аналитических документов; методами управления информационной безопасностью и методами ввода в эксплуатацию информационных систем.	
		БАЗОВЫЙ	*Выпускник знает:* на достаточном уровне порядок проведения аттестации объектов информационной защиты; типовые методики испытаний объектов информатизации по требованиям защиты информации; системы и средства обеспечения информационной безопасности, необходимые для организации выполнения работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности сведения; методологию создания систем защиты информации; перспективные направления развития средств и методов защиты информации; основные положения существующей законодательной базы и нормативные документы в области информационной безопасности; методы аттестации уровня защищенности информационных систем. *Выпускник умеет:* на достаточном уровне определять угрозы объекту информатизации; определять рациональные способы и средства защиты информации на объекте информатизации; организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности; организовать технологический процесс защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю; определять комплекс мер для обеспечения ввода в эксплуатацию систем информационной безопасности. *Выпускник владеет:* на достаточном уровне навыками и опы-	4

			том организации мероприятий по защите информации на объекте информатизации; навыками введения в эксплуатацию систем и средств обеспечения информационной безопасности; навыками работы с нормативными документами; правилами составления локальных нормативных актов и регламентов в области информационной безопасности; навыками подготовки отчетных и аналитических документов; методами управления информационной безопасностью и методами ввода в эксплуатацию информационных систем.	
		ПОРОГОВЫЙ	*Выпускник знает:* на допустимом уровне порядок проведения аттестации объектов информационной защиты; типовые методики испытаний объектов информатизации по требованиям защиты информации; системы и средства обеспечения информационной безопасности, необходимые для организации выполнения работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности сведения; методологию создания систем защиты информации; перспективные направления развития средств и методов защиты информации; основные положения существующей законодательной базы и нормативные документы в области информационной безопасности; методы аттестации уровня защищенности информационных систем. *Выпускник умеет:* на допустимом уровне определять угрозы объекту информатизации; определять рациональные способы и средства защиты информации на объекте информатизации; организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности; организовать технологический процесс защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю; определять комплекс мер для обеспечения ввода в эксплуатацию систем информационной безопасности. *Выпускник владеет:* на допустимом уровне навыками и опытом организации мероприятий по защите ин-	3

			формации на объекте информатизации; навыками введения в эксплуатацию систем и средств обеспечения информационной безопасности; навыками работы с нормативными документами; правилами составления локальных нормативных актов и регламентов в области информационной безопасности; навыками подготовки отчетных и аналитических документов; методами управления информационной безопасностью и методами ввода в эксплуатацию информационных систем.	
ПК-16	Способностью разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности	ПОВЫШЕННЫЙ	*Выпускник знает:* на высоком уровне требования и особенности реализации правовых нормативных актов и нормативных методических документов ФСБ России, ФСТЭК России; специальную научно-техническую литературу; основы разработки проектов организационно-распорядительной документации в сфере защиты информации; современные информационные технологии, используемые в управлении проектами; методику разработки организационно-распорядительных документов, бизнес-планов в сфере информационной безопасности, стандарты оформления организационно-распорядительных документов; сертифицированные продукты защиты информации. *Выпускник умеет:* на высоком уровне формировать технические задания и участвовать в разработке или модернизации средств и средств обеспечения информационной безопасности; анализировать и оптимизировать созданные проектные решения; разрабатывать проекты организационно-распорядительных документов на системы и средства обеспечения информационной безопасности; формировать организационную структуру для реализации проекта; разрабатывать проекты организационно-распорядительных документов в сфере профессиональной деятельности; использовать техническую и эксплуатационную документацию на системы и средства обеспечения информационной безопасности; использовать сертифицированные продукты защиты информации. *Выпускник владеет:* на высоком уровне представлением о методологиях и подходах к разработке опти-	5

			мальных решений по защите информации с учетом требований руководящих документов; специальными программными средствами для разработки проектов организационно-распорядительных документов в сфере защиты информации; навыками организации контроля хода реализации проекта; навыками разработки технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности; навыками разработки проектов организационно-распорядительных документов в сфере профессиональной деятельности; навыками проведения бенчмаркинга информационной безопасности; методиками построения защиты информации на предприятиях.	
		БАЗОВЫЙ	*Выпускник знает:* на достаточном уровне требования и особенности реализации правовых нормативных актов и нормативных методических документов ФСБ России, ФСТЭК России; специальную научно-техническую литературу; основы разработки проектов организационно-распорядительной документации в сфере защиты информации; современные информационные технологии, используемые в управлении проектами; методику разработки организационно-распорядительных документов, бизнес-планов в сфере информационной безопасности, стандарты оформления организационно-распорядительных документов; сертифицированные продукты защиты информации. *Выпускник умеет:* на достаточном уровне формировать технические задания и участвовать в разработке или модернизации средств и средств обеспечения информационной безопасности; анализировать и оптимизировать созданные проектные решения; разрабатывать проекты организационно-распорядительных документов на системы и средства обеспечения информационной безопасности; формировать организационную структуру для реализации проекта; разрабатывать проекты организационно-распорядительных документов в сфере профессиональной деятельности; использовать техническую и эксплуатационную документацию на системы и средства обеспечения информационной безопасно-	4

			сти; использовать сертифицированные продукты защиты информации. *Выпускник владеет:* на достаточном уровне представлением о методологиях и подходах к разработке оптимальных решений по защите информации с учетом требований руководящих документов; специальными программными средствами для разработки проектов организационно-распорядительных документов в сфере защиты информации; навыками организации контроля хода реализации проекта; навыками разработки технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности; навыками разработки проектов организационно-распорядительных документов в сфере профессиональной деятельности; навыками проведения бенчмаркинга информационной безопасности; методиками построения защиты информации на предприятиях.	
		ПОРОГОВЫЙ	*Выпускник знает:* на допустимом уровне требования и особенности реализации правовых нормативных актов и нормативных методических документов ФСБ России, ФСТЭК России; специальную научно-техническую литературу; основы разработки проектов организационно-распорядительной документации в сфере защиты информации; современные информационные технологии, используемые в управлении проектами; методику разработки организационно-распорядительных документов, бизнес-планов в сфере информационной безопасности, стандарты оформления организационно-распорядительных документов; сертифицированные продукты защиты информации. *Выпускник умеет:* на допустимом уровне формировать технические задания и участвовать в разработке или модернизации средств и средств обеспечения информационной безопасности; анализировать и оптимизировать созданные проектные решения; разрабатывать проекты организационно-распорядительных документов на системы и средства обеспечения информационной безопасности; формировать организационную структуру для реализации проекта; разрабатывать проекты организационно-	3

			распорядительных документов в сфере профессиональной деятельности; использовать техническую и эксплуатационную документацию на системы и средства обеспечения информационной безопасности; использовать сертифицированные продукты защиты информации. *Выпускник владеет:* на допустимом уровне представлением о методологиях и подходах к разработке оптимальных решений по защите информации с учетом требований руководящих документов; специальными программными средствами для разработки проектов организационно-распорядительных документов в сфере защиты информации; навыками организации контроля хода реализации проекта; навыками разработки технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности; навыками разработки проектов организационно-распорядительных документов в сфере профессиональной деятельности; навыками проведения бенчмаркинга информационной безопасности; методиками построения защиты информации на предприятиях.	

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 относится к блоку (Б.3) «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. Создание инфраструктуры обработки и защиты информации с использованием технологий виртуализации.

11. Разработка методики цифровой обработки сигналов в системах информационной безопасности.

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

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

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

15. Разработка информационной системы для ведения реестра значимых объектов критическое информационной инфраструктуры.

16. Организация и обеспечение информационной безопасности образовательного Интернета вещей.

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

18. Создание виртуальной лаборатории компьютерной безопасности.

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

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

21. Комплексная система защиты информации на примере предприятия Х.

22. Совершенствование управления информационной безопасностью в организации.

23. Совершенствование информационной безопасности в организации.

24. Разработка персонального межсетевого экрана с изолированным ядром.

25. Проектирование защищенной сети передачи данных предприятия Х.

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

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

28. Комплексная система защиты электронного документооборота.

29. Исследования методов защиты информации в сетях передачи данных.

30. Исследование уязвимостей алгоритмов защиты информации.

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

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

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

34. Эффективность затрат на информационную безопасность в организации.

35. 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, технологий защиты информации, систем управления информационной безопасностью.

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 формируемой компетенции	Часть ГИА, в которой проводится оценка уровня сформированности компетенции
ОК-1	способностью к абстрактному мышлению, анализу, синтезу	Отзыв руководителя рецензия, текст ВКР, защита ВКР
ОК-2	способностью самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения	Отзыв руководителя рецензия, текст ВКР, защита ВКР
ОПК-1	способностью к коммуникации в устной и письменной формах на государственном и одном из иностранных языков для решения задач профессиональной деятельности	Отзыв руководителя рецензия, текст ВКР, защита ВКР
ОПК-2	способностью к самостоятельному обучению и применению новых методов исследования профессиональной деятельности	Отзыв руководителя рецензия, текст ВКР, защита ВКР
ПК-1	способностью анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты	Отзыв руководителя рецензия, текст ВКР, защита ВКР
ПК-2	способностью разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности	Отзыв руководителя рецензия, текст ВКР, защита ВКР
ПК-3	способностью проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов	Отзыв руководителя, рецензия, текст ВКР, защита ВКР
ПК-4	способностью разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности	Отзыв руководителя, рецензия, текст ВКР
ПК-5	способностью анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества	Отзыв руководителя, рецензия, текст ВКР
ПК-6	способностью осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методов и средств решения задачи, разрабатывать планы и программы проведения научных иссле-	Отзыв руководителя, рецензия, текст ВКР, защита ВКР

	дований и технических разработок	
ПК-7	способностью проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента	Отзыв руководителя, рецензия, текст ВКР, защита ВКР
ПК-8	способностью обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи	Отзыв руководителя, рецензия, текст ВКР, защита ВКР
ПК-12	способностью организовать выполнение работ, управлять коллективом исполнителей и принимать управленческие решения	Отзыв руководителя, рецензия, текст ВКР, защита ВКР
ПК-13	способностью организовать управление информационной безопасностью	Отзыв руководителя, рецензия, текст ВКР
ПК-14	способностью организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России	Отзыв руководителя, рецензия, текст ВКР, защита ВКР
ПК-15	способностью организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности	Отзыв руководителя, рецензия, текст ВКР, защита ВКР
ПК-16	способностью разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности	Отзыв руководителя, рецензия, текст ВКР, защита 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»)
ОК-1	способностью к абстрактному мышлению, анализу, синтезу	
ОК-2	способностью самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения	
ОПК-1	способностью к коммуникации в устной и письменной формах на государственном и одном из иностранных языков для решения задач профес-	

	сиональной деятельности	
ОПК-2	способностью к самостоятельному обучению и применению новых методов исследования профессиональной деятельности	
ПК-1	способностью анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты	
ПК-2	способностью разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности	
ПК-3	способностью проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов	
ПК-4	способностью разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности	
ПК-5	способностью анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества	
ПК-6	способностью осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методов и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок	
ПК-7	способностью проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента	
ПК-8	способностью обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи	
ПК-12	способностью организовать выполнение работ, управлять коллективом исполнителей и принимать управленческие решения	
ПК-13	способностью организовать управление информационной безопасностью	
ПК-14	способностью организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России	
ПК-15	способностью организовать выполнение работ по вводу в эксплуатацию систем и средств обеспече-	

	ния информационной безопасности	
ПК-16	способностью разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности	
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 дан-

ными 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)				
ОК-1, ОК-2, ОПК-1, ОПК-2, ПК-6, ПК-14, ПК-16	Использование литературы (достаточное количество актуальных источников, достаточность цитирования, использование нормативных документов, научной и справочной литературы)	повышенный	базовый	пороговый
ПК-16	Соответствие ВКР нормативным локальным актам «Государственная итоговая аттестация выпускников СГУГиТ. Структура и правила оформления», «Положение о порядке проведения проверки письменных работ на наличие заимствований»	повышенный	базовый	пороговый
Средний балл				
2. Показатели оценки по содержанию (пример)				
ОК-2, ПК-1, ПК-5, ПК-6, ПК-14, ПК-16	Введение содержит следующие обязательные элементы: актуальность темы и практическая значимость работы; цель ВКР, соответствующая заявленной теме; круг взаимосвязанных задач, определенных	повышенный	базовый	пороговый

	поставленной целью			
ОК-1, ОК-2, ОПК-1, ОПК-2, ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-6, ПК-7, ПК-8, ПК-12, ПК-13, ПК-14, ПК-15, ПК-16	Содержательность и глубина теоретической, научно-исследовательской и практической проработки проблемы	повышенный	базовый	пороговый
ОПК-2, ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-6, ПК-7, ПК-8, ПК-12, ПК-13, ПК-14, ПК-15, ПК-16	Содержательность производственно-технологической характеристики объекта исследования и глубина проведённого анализа проблемы. Качество анализа проблемы, планирование и осуществление деятельности в области	повышенный	базовый	пороговый
ОПК-2, ПК-2, ПК-3, ПК-4, ПК-5, ПК-6, ПК-7, ПК-8, ПК-12, ПК-13, ПК-14, ПК-15, ПК-16	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	повышенный	базовый	пороговый
ОК-1, ОК-2, ОПК-2, ПК-1, ПК-2, ПК-3, ПК-4, ПК-6, ПК-8, ПК-12, ПК-13, ПК-14, ПК-15, ПК-16	Оригинальность и практическая значимость предложений и рекомендаций	повышенный	базовый	пороговый
Средний балл				
3. Показатели оценки защиты ВКР				
ОК-1, ОК-2, ОПК-2, ПК-5, ПК-6, ПК-8, ПК-14, ПК-16	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	повышенный	базовый	пороговый
ОК-2, ОПК-2, ПК-8, ПК-16	Качество и использование презентационного материала (информативность, соответствие содержанию доклада, наглядность, достаточность)	повышенный	базовый	пороговый
ОПК-1, ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-6, ПК-8, ПК-14, ПК-16	Ответы на вопросы комиссии (полнота, глубина, оригинальность мышления. Общий уровень культуры общения с аудиторией	повышенный	базовый	пороговый
Средний балл				
Итоговая оценка	*Примечание: оценка «отлично» выставляется, если средний балл по всем*			

члена ГЭК	*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: 19.06.2022). — 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: 19.06.2022). — 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: 19.06.2022). – 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: 15.06.2022). – 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: https://e.lanbook.com/book/123703 (дата обращения: 19.06.2022). — Режим доступа: для авториз. пользователей.	Электронный ресурс
6.	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: 19.06.2022). —	Электронный ресурс

	Режим доступа: для авториз. пользователей.	
7.	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: 06.06.2022). — Режим доступа: для авториз. пользователей.	Электронный ресурс
8.	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: 06.06.2022). — Режим доступа: для авториз. пользователей.	Электронный ресурс
9.	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
10.	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: 06.07.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
11.	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: 16.06.2022). – Режим доступа: по подписке.	Электронный ресурс
12.	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: 16.06.2022). — Режим доступа: для авториз. пользователей.	Электронный ресурс
13.	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: 07.06.2022). — Режим доступа: для авториз. пользователей.	Электронный ресурс
14.	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: 06.06.2022). – Режим доступа: по подписке.	Электронный ресурс
15.	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: 06.06.2022). — Режим доступа: для авториз. пользователей.	Электронный ресурс
16.	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 : электрон-	Электронный ресурс

	но-библиотечная система. — URL: https://e.lanbook.com/book/180099 (дата обращения: 06.06.2022). — Режим доступа: для авториз. пользователей.	
17.	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: 16.06.2022). — Режим доступа: для авториз. пользователей.	Электронный ресурс
18.	Овчаров, А. О. Методология научного исследования : учебник / А.О. Овчаров, 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: 16.06.2022). – Режим доступа: по подписке.	Электронный ресурс
19.	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: 19.06.2022). — Режим доступа: для авториз. пользователей.	Электронный ресурс
20.	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: 16.06.2022). — Режим доступа: для авториз. пользователей.	Электронный ресурс
21.	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: 06.06.2022). – Режим доступа: по подписке.	Электронный ресурс
22.	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: 06.06.2022). — Режим доступа: для авториз. пользователей.	Электронный ресурс
23.	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: 06.06.2022). — Режим доступа: для авториз. пользователей.	Электронный ресурс
24.	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: 06.06.2022). — Режим доступа: для авториз. пользователей.	Электронный ресурс
25.	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. — ISBN 978-5-8114-8064-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/171422 (дата обращения: 06.06.2022). — Режим доступа: для авториз. пользователей.	Электронный ресурс

26.	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: 06.06.2022). — 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: 06.06.2022). — 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: 06.06.2022). — 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: 15.06.2022). – Режим доступа: по подписке.	Электронный ресурс
4.	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: 16.06.2022). — Режим доступа: для авториз. пользователей.	Электронный ресурс
5.	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: 16.06.2022)	Электронный ресурс
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: 10.06.2022). — 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: 10.06.2022). — Режим доступа: для авториз. пользователей.	Электронный ресурс

8.	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: 20.06.2022). – Режим доступа: по подписке.	Электронный ресурс
9.	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: 20.06.2022— Режим доступа: для авториз. пользователей.	Электронный ресурс
10.	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: 16.06.2022). — Режим доступа: для авториз. пользователей.	Электронный ресурс
11.	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: 17.06.2022). — Режим доступа: для авториз. пользователей.	Электронный ресурс
12.	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
13.	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: 17.06.2022). — Режим доступа: для авториз. пользователей.	Электронный ресурс
14.	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: 16.06.2022). — Режим доступа: для авториз. пользователей.	Электронный ресурс
15.	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: 17.06.2022). — Режим доступа: для авториз. пользователей.	Электронный ресурс
16.	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: 16.06.2022). — Режим доступа: для авториз. пользователей.	Электронный ресурс
17.	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	Электронный ресурс

	система. — URL: https://e.lanbook.com/book/111057 (дата обращения: 17.06.2022). — Режим доступа: для авториз. пользователей.	
18.	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: 17.06.2022). — Режим доступа: для авториз. пользователей.	Электронный ресурс
19.	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: 17.06.2022). — Режим доступа: для авториз. пользователей.	Электронный ресурс
20.	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: 17.06.2022). — Режим доступа: для авториз. пользователей.	Электронный ресурс
21.	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: 15.06.2022). – Режим доступа: по подписке.	Электронный ресурс
22.	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: 15.06.2022). – Режим доступа: по подписке.	Электронный ресурс
23.	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: 16.06.2022). — Режим доступа: для авториз. пользователей.	Электронный ресурс
24.	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: 16.06.2022). – Режим доступа: по подписке.	Электронный ресурс
25.	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: 15.06.2022). – Режим доступа: по подписке.	Электронный ресурс
26.	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

27.	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
28.	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: 19.06.2022). — Режим доступа: для авториз. пользователей.	Электронный ресурс
29.	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: 19.06.2022). — Режим доступа: для авториз. пользователей.	Электронный ресурс
30.	Методы защищенного управления информационнообразовательными фондами вузов : монография / С. Г. Фомичева, С. В. Беззатеев, Т. Н. Елина, 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: 19.06.2022). — Режим доступа: для авториз. пользователей.	Электронный ресурс
31.	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
32.	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: 15.06.2022). — Режим доступа: для авториз. пользователей.	Электронный ресурс
33.	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
34.	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: 15.06.2022). — Режим доступа: для авториз. пользователей.	Электронный ресурс
35.	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
36.	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: 15.06.2022). — Режим доступа: для авториз. пользователей.	Электронный ресурс

37.	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: 16.07.2022). — Режим доступа: для авториз. пользователей.	Электронный ресурс
38.	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
39.	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: 20.07.2022). — Режим доступа: для авториз. пользователей.	Электронный ресурс
40.	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: 06.07.2022). — Режим доступа: для авториз. пользователей.	Электронный ресурс
41.	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: 16.07.2022). – Режим доступа: по подписке.	Электронный ресурс
42.	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: 06.07.2022). — Режим доступа: для авториз. пользователей.	Электронный ресурс
43.	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: 06.07.2022). — Режим доступа: для авториз. пользователей.	Электронный ресурс
44.	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: 06.07.2022). — Режим доступа: для авториз. пользователей.	Электронный ресурс
45.	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: 06.07.2022). — Режим доступа: для авториз. пользователей.	Электронный ресурс
46.	Риск и рефлексия : монография / В. П. Балан, С. А. Баркалов, А. В. Душкин [и др.] ; под общей редакцией В. И. Новосельцева. — Москва : Горя-	Электронный ресурс

	чая 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: 20.07.2022). — Режим доступа: для авториз. пользователей.	
47.	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: 20.07.2022). — Режим доступа: для авториз. пользователей.	Электронный ресурс
48.	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: 06.07.2022). — Режим доступа: для авториз. пользователей.	Электронный ресурс
49.	Теоретические основы управления в организациях [Электронный ресурс] : 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	Электронный ресурс
50.	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: 15.07.2022). – Режим доступа: по подписке.	Электронный ресурс
51.	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: 06.07.2022). — Режим доступа: для авториз. пользователей.	Электронный ресурс
52.	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: 06.07.2022). — Режим доступа: для авториз. пользователей.	Электронный ресурс
53.	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: 06.07.2022). – Режим доступа: по подписке.	Электронный ресурс
54.	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: 06.07.2022). — Режим доступа: для авториз. пользователей.	Электронный ресурс
55.	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	Электронный ресурс

	обращения: 06.07.2021). — Режим доступа: для авториз. пользователей.	
56.	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: 06.07.2022). — Режим доступа: для авториз. пользователей.	Электронный ресурс
57.	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: 06.07.2022). — Режим доступа: для авториз. пользователей.	Электронный ресурс
58.	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: 20.07.2022). – Режим доступа: по подписке.	Электронный ресурс
59.	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: 19.07.2022). — Режим доступа: для авториз. пользователей.	Электронный ресурс
60.	Требования к средствам антивирусной защиты. Утверждены приказом ФСТЭК России от 20.03.2012 № 28. Инв. № 891. ДСП	1
61.	Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждено ФСТЭК России 25.12.2006. ДСП	1
62.	Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждено ФСТЭК России 15.02.2008. ДСП	1
63.	Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждено ФСТЭК России 15.02.2008. ДСП	1
64.	Основные мероприятия по организации и обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных. Утверждено ФСТЭК России 15.02.2008. ДСП	1
65.	Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждено ФСТЭК России 15.02.2008. ДСП	1
66.	Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638. ДСП	1
67.	Требования в области технического регулирования к продукции, используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа (требования к средствам доверенной загрузки). Утверждены приказом ФСТЭК России от 27 сентября 2013 г. № 119. ДСП	1
68.	Требования к обеспечению защиты информации, содержащейся в информационных системах управления производством, используемых организациями оборонно-промышленного комплекса. Утверждены приказом ФСТЭК России от 28 февраля 2017 г. № 31. ДСП	1

69.	Требования к средствам контроля съемных машинных носителей информации. Утверждены приказом ФСТЭК России от 28 июля 2014 г. № 87. ДСП	1
70.	Требования к межсетевым экранам. Утверждены приказом ФСТЭК России от 9 февраля 2016 г. № 9. ДСП	1
71.	Требованиям безопасности информации к операционным системам, утвержденным приказом ФСТЭК России от 19 августа 2016 г. № 119. ДСП	1
72.	Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий, утвержденным приказом ФСТЭК России от 2 июня 2020 г. № 76. ДСП	1
73.	Сборник методических документов по технической защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в волоконно-оптических системах передачи (МД по ТЗИ ВОСП-К). Утвержден приказом ФСТЭК России от 15 марта 2012 г. № 27. ДСП	1
74.	Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Гостехкомиссия России. Москва: 2002 – 74 с. ДСП	1
75.	Методика выявления уязвимостей и недекларированных возможностей в программном обеспечении. Утверждена ФСТЭК России 11 февраля 2019 г. ДСП	1
76.	Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282. ДСП	1

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 ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства

обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий.

13 ГОСТ Р ИСО/МЭК ТО 18044-2007 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности.

14 ГОСТ Р ИСО/МЭК 18045-2013 Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий.

15 ГОСТ Р ИСО/МЭК 27001-2021 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

16 ГОСТ Р ИСО/МЭК 27003-2021 Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации.

17 ГОСТ Р ИСО/МЭК 27004-2021 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Мониторинг, оценка защищенности, анализ и оценивание.

18 ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности (взамен ГОСТ Р ИСО/МЭК ТО 13335-3-2007 и ГОСТ Р ИСО/МЭК ТО 13335-4-2007).

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).