МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Сибирский государственный университет геосистем и технологий»
(СГУГиТ)
Кафедра информационной безопасности

ПРОГРАММА ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

Направление подготовки
10.04.01 Информационная безопасность

Профиль подготовки
Организация и управление информационной безопасностью

Квалификация (степень) выпускника
Магистр

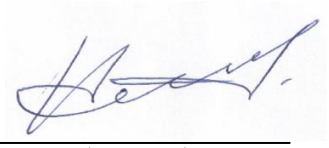
Форма обучения
Очная, очно-заочная

Новосибирск, 2020

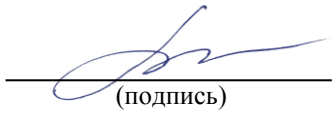
Программа государственной итоговой аттестации по направлению подготовки магистров 10.04.01 Информационная безопасность составлена на основании федерального государственного образовательного стандарта высшего образования, утвержденного приказом Министерства образования и науки Российской Федерации от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

Составители:
Новиков С.Н., заведующий кафедрой информационной безопасности, д.т.н., доцент

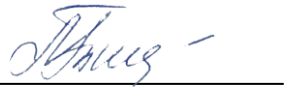
Программа государственной итоговой аттестации обсуждена и одобрена на заседании кафедры информационной безопасности (ИБ).

Зав. кафедрой ИБ  *С.Н. Новиков*
(подпись)

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

Председатель ученого совета ИОиТИБ  *А.В. Шабурова*
(подпись)

«СОГЛАСОВАНО»

Зав. библиотекой  *Л.А. Тимофеева*
(подпись)

ОГЛАВЛЕНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

Государственная итоговая аттестация (далее – ГИА) представляет собой форму оценки степени и уровня освоения обучающимися основной образовательной программы (далее – ООП), 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 локальным нормативным актом СГУГиТ.

К ГИА допускаются обучающиеся, не имеющие академической задолженности и в полном объеме выполнившие учебный план или индивидуальный учебный план.

Обучающимся, успешно прошедшим ГИА, выдается документ об образовании и о квалификации образца, установленного Министерством образования и науки Российской Федерации.

Обучающиеся, не прошедшие ГИА или получившие на ГИА неудовлетворительные результаты, вправе пройти ГИА в сроки, определяемые порядком проведения ГИА по соответствующим основным образовательным программам (далее – ООП).

К проведению ГИА по ООП привлекаются представители работодателей или их объединений.

2. ЦЕЛИ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

ГИА проводится государственными экзаменационными комиссиями в целях определения соответствия результатов освоения обучающимися основных образовательных программ соответствующим требованиям федерального государственного образовательного стандарта по направлению подготовки 10.04.01 Информационная безопасность (уровень магистратура), профиль «Организация и управление информационной безопасностью».

Задачами ГИА являются:

– оценка степени и уровня освоения обучающимися основных образовательных программ 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, в форме практической подготовки, предусмотренных учебным планом по направлению подготовки 10.04.01 Информационная безопасность (уровень магистратура), профиль «Организация и управление информационной безопасностью».

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

Трудоемкость ГИА составляет 6 зачетных единиц (216 академических часов) и проводится, согласно учебному плану по очной форме обучения – на 2 курсе, очно-заочной форме – на 3 курсе обучения.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

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

В результате освоения ООП у выпускника должны быть сформированы следующие компетенции:

Таблица 1

Перечень компетенций

Код компетенции	Содержание формируемой компетенции
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 профессиональной 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 обеспечения 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

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

Шкала оценивания	Критерии оценивания
«отлично»	обучающийся должен: продемонстрировать глубокое и прочное усвоение знаний материала; исчерпывающе, последовательно, грамотно и логически стройно изложить теоретический материал; правильно формулировать определения; продемонстрировать умения самостоятельной работы с нормативно- правовой литературой; уметь сделать выводы по излагаемому материалу
«хорошо»	обучающийся должен: продемонстрировать достаточно полное знание материала; продемонстрировать знание основных теоретических понятий; достаточно последовательно, грамотно и логически стройно излагать материал; продемонстрировать умение ориентироваться в нормативно-правовой литературе; уметь сделать достаточно обоснованные выводы по излагаемому материалу
«удовлетворительно»	обучающийся должен: продемонстрировать общее знание изучаемого материала; знать основную рекомендуемую программой дисциплины учебную литературу; уметь строить ответ в соответствии со структурой излагаемого вопроса; показать общее владение понятийным аппаратом дисциплины

Таблица 3

Критерии определения сформированности компетенций

	Уровни сформированности компетенций		
	Пороговый	Базовый	Повышенный
Критерии	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

Таблица 4

Уровни сформированности компетенций

Формируемая компетенция	Уровень сформированности компетенции	Оценивание «знать», «уметь», «владеть»	Шкала оценивания
ОК-1 - способностью к абстрактному мышлению, анализу, синтезу	ПОВЫШЕННЫЙ	Знать: 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). Уметь: 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. Владеть: 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	Знать: 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). Уметь: 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. Владеть: 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.	4

	ПОРОГОВЫЙ	Знать: 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). Уметь: 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. Владеть: 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 новые знания и умения	ПОВЫШЕННЫЙ	Знать: 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 деятельности в образовании; особенности диссертационного исследования как вида научно-исследовательской работы. Уметь: 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. Владеть: 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	5
	БАЗОВЫЙ	Знать: на достаточном уровне современ-	4

		ные 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. Уметь: 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. Владеть: навыками построения защиты ОС Windows, Unix; навыками планирования научного исследования, анализа получаемых результатов и формулировки выводов; спецификой научно-исследовательской работы с достаточной адаптивностью практического навыка.	
	ПОРОГОВЫЙ	Знать: 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. Уметь: 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. Владеть: навыками построения защиты ОС Windows, Unix; навыками планирования научного исследования, анализа получаемых результатов и формулировки выво-	3

		дов; спецификой научно-исследовательской работы с допустимой адаптивностью практического навыка.	
ОПК-1 - способностью к коммуникации в устной и письменной формах на государственном и одном из иностранных языков для решения задач профессиональной деятельности	ПОВЫШЕННЫЙ	Знать: 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. Уметь: 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; пользоваться основной справочной литературой, толковыми и нормативными словарями. Владеть: 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.	5
	БАЗОВЫЙ	Знать: 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. Уметь: 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;	4

		пользоваться основной справочной литературой, толковыми и нормативными словарями**.** Владеть: 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.	
	ПОРОГОВЫЙ	Знать: на допустимом 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. Уметь: 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**.** Владеть: 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.	3
ОПК-2 - способностью к самостоятельному обучению и применению новых методов исследования профессиональной деятельности	ПОВЫШЕННЫЙ	Знать: 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	5

		профессиональной деятельности. Уметь: 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 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. Владеть 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	Знать: 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. Уметь: на достаточном уровне анализировать состояние научно-технической проблемы в профессиональной области деятельности и на этой основе определить цель исследования, методы и средства ее	4

		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. Владеть: 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	Знать: 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. Уметь: 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 ре-	3

		зультаты, 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. Владеть: 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	Знать: 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. Уметь: 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 без-	5

		опасности 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. Владеть: 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	Знать: 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	4

		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. Уметь: 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. Владеть: 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 использо-	

		вании 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.	
	ПОРОГОВЫЙ	Знать: 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. Уметь: 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

		Владеть: 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	Знать: 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. Уметь: на высоком 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 обеспече-	5

		ния 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; Владеть: 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	Знать: 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. Уметь: на достаточном уровне разрабатывать системы для контроля защищенности информации от утечки и от несанкционированного доступа; проводить общенауч-	4

		ные 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; Владеть: 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	Знать: 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 каналы утечки информации; возможности технических разведок; способы и методы научного исследования в профессиональной сфере; системы, комплексы, средства и технологии обеспечения информационной безопасности.	3

		Уметь: 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; Владеть: 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 средств обеспечения информационной безопасности объектов защиты на основе россий-	ПОВЫШЕННЫЙ	Знать: 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 безопасности; российские и международные стандарты в сфере информационной безопасности; нормативно-правовые документы в области информационной безопасности, используемые для определения характеристик и функциональных возможностей систем. Уметь: на высоком уровне проводить	5

ских и международных стандартов		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 Владеть: 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	Знать: 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 безопасности, используемые для определения характеристик и функциональных возможностей систем. Уметь: 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	4

		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 Владеть: 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	Знать: 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. Уметь: 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	3

		систем и средств обеспечения информационной безопасности Владеть: 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	Знать: 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 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. Уметь: на высоком уровне проводить аудит информационной безопасности предприятий, организаций вне зависимости от их формы собственности и сферы деятельности; проводить испытания средств информационной безопасности;	5

		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. Владеть: 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 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.	
	БАЗОВЫЙ	Знать: 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 защит-	4

		ные 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. Уметь: 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 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. Владеть: 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	Знать: 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 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 без-	3

		опасности. Уметь: 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. Владеть: 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 докумен-	

		тами.	
ПК- 5 - способностью анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества	ПОВЫШЕННЫЙ	Знать: 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. Уметь: на высоком уровне уверенно 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. Владеть: на высоком уровне навыками критического анализа и оценки современных научных достижений и результатов деятельности по решению исследователь-	5

		ских 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	Знать: 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; 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. Уметь: 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 интерпретиро-	4

		вать 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**.** Владеть: 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 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.	
	ПОРОГОВЫЙ	Знать: 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	3

		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. Уметь: 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 становления современного информационного общества; выявлять различные сценарии развития рисковых ситуаций в информационном пространстве**.** Владеть: 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 - способ-	ПОВЫШЕННЫЙ	Знать: на высоком уровне способы сбора,	5

ностью 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		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. Уметь: 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 комплексной безопасности в организации; использовать методы экономики при определении эффективности вложений в систему комплексной безопасности в организации Владеть: 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	Знать: 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 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; тех-	4

		нологию аналитических исследований информационного пространства субъектов экономической деятельности. Уметь: 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 Владеть: 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	Знать: 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 прове-	3

		дения 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. Уметь: 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 прове-	

		дение 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 Владеть: 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; 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.	
ПК-7 - способностью проводить экспери-	ПОВЫШЕННЫЙ	Знать: на высоком уровне физические и математические методы исследования защищенности объектов; методы экспери-	5

ментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента		ментальных 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. Уметь: 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. Владеть: на высоком уровне навыками применения технических и программных средств обработки результатов эксперимента; средствами обработки результатов исследований по выявлению каналов несанкционированного доступа и утечки ин-	

		формации; 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	Знать: 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. Уметь: 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	4

		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. Владеть: 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	Знать: 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	3

		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. Уметь: на допустимом 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. Владеть: 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, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи	ПОВЫШЕННЫЙ	Знать: 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); 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. Уметь: 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	5

		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. Владеть: 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	Знать: 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 под-	4

		готовки 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. Уметь: 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. Владеть: 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 науч-	

		ных 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.	
	ПОРОГОВЫЙ	Знать: 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. Уметь: 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 информаци-	3

		онной 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. Владеть: 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	Знать: 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 си-	5

		стем; процессы и процедуры планирования системы управления информационной безопасностью. Уметь: 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. Владеть: 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	Знать: 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. Уметь: на достаточном уровне выбирать рациональные методы и средства управления проектом; принимать управленческие решения для защиты информационного пространства предприятий; организовать выполнение работ, связанных с монито-	4

		рингом внешней среды и внутренних показателей; управлять коллективом и принимать управленческие решения с учетом жизненного цикла информационных систем; использовать рискориентированную методологию управления информационной безопасностью. Владеть: 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	Знать: 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. Уметь: 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. Владеть: на допустимом уровне навыками формирования графика хода реализации	3

		проекта; навыками управления коллективом исполнителей для решения задач защиты 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	Знать: 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. Уметь: 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 информационной безопасности с учетом специфики этих объектов Владеть: на высоком уровне навыками	5

		управления системой информационной безопасности; навыками управления коллективом исполнителей решения задач защиты 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	Знать: 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. Уметь: 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 информации для использования их с целью обеспечения требуемого уровня защищённости; прогнозировать эффективность функционирования информационных техноло-	4

		гий, оценивать затраты и риски в сфере информационной безопасности с учетом специфики этих объектов Владеть: на достаточном уровне навыками управления системой информационной безопасности; навыками управления коллективом исполнителей решения задач защиты 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	Знать: 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. Уметь: на допустимом 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-	3

		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 Владеть: 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	Знать: 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. Уметь: 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 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	5

		экспортному контролю Владеть: 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	Знать: 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. Уметь: 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, Федеральной службой по техническому и экспортному контролю Владеть: 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 документа-	4

		ции 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	Знать: 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. Уметь: 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 Владеть: на допустимом 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	3

		по техническому и экспортному контролю	
ПК-15 - способностью организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности	ПОВЫШЕННЫЙ	Знать: 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. Уметь: 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. Владеть: 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.	5
	БАЗОВЫЙ	Знать: на достаточном уровне порядок проведения аттестации объектов информационной защиты; типовые методики испы-	4

		таний 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. Уметь: 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. Владеть: на достаточном 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.	
	ПОРОГОВЫЙ	Знать: на допустимом уровне порядок проведения аттестации объектов информационной защиты; типовые методики испытаний объектов информатизации по требованиям защиты информации; системы и средства обеспечения информационной	3

		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. Уметь: 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. Владеть: на допустимом 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.	
ПК-16 - способностью разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере	ПОВЫШЕННЫЙ	Знать: 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 техноло-	5

профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности		гии, используемые в управлении проектами; методику разработки организационно-распорядительных документов, бизнес-планов в сфере информационной безопасности, стандарты оформления организационно-распорядительных документов; сертифицированные продукты защиты информации. Уметь: 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. Владеть: на высоком 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.	
	БАЗОВЫЙ	Знать: 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	4

		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. Уметь: 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 безопасности; использовать сертифицированные продукты защиты информации. Владеть: 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	Знать: на допустимом уровне требования и особенности реализации правовых нормативных актов и нормативных методиче-	3

		ских 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. Уметь: 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-распорядительных документов в сфере профессиональной деятельности; использовать техническую и эксплуатационную документацию на системы и средства обеспечения информационной безопасности; использовать сертифицированные продукты защиты информации. Владеть: 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.	

4. МЕСТО ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ В СТРУКТУРЕ ООП

Государственная итоговая аттестация относится к блоку (Б.3) «Государственная итоговая аттестация»

Предшествующие (обеспечивающие) дисциплины, практики:

Защищенные информационные системы

Технологии обеспечения информационной безопасности

Управление информационной безопасностью

Методология научных исследований

Иностранный язык в профессиональной деятельности

Проектный менеджмент

Научно-технический семинар

Управление рисками информационной безопасности

Аттестация объектов информатизации по требованиям безопасности информации

Защита в операционных системах

Отечественные и зарубежные стандарты в области информационной безопасности

Аудит информационных систем и объектов информатизации

Проектирование защищенных телекоммуникационных систем

Специальные главы цифровой обработки изображений

Технические, организационные и кадровые аспекты управления информационной безопасностью

Управление жизненным циклом информационных систем

Проектирование организационно-распорядительной документации в сфере профессиональной деятельности

Программы и методики испытаний средств и систем обеспечения информационной безопасности

Контроль защищенности информации от несанкционированного доступа

Контроль защищенности информации от утечки по техническим каналам

Разработка управленческих решений

Интеллектуальная собственность и патентоведение

Производственная практика: практика по получению профессиональных умений и опыта профессиональной деятельности в форме практической подготовки

Производственная практика: научно-исследовательская работа (НИР) в форме практической подготовки

Производственная практика: преддипломная практика в форме практической подготовки

Государственная итоговая аттестация проводится по очной форме обучения на 2 курсе в 4 семестре, очно-заочной форме – на 3 курсе обучения в 5-м семестре. Общий объем в программе подготовки магистров, отведенный на ГИА, составляет 6 з.е., 216 часов.

5. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

5.1. Методические указания по подготовке к ВКР

Выпускная квалификационная работа (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) 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.

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 выпускной квалификационной работе проявляются: уровень фундаментальной и специальной подготовки обучающегося; его способность к анализу и обобщению изученного материала в соответствии с поставленной задачей, умение проектировать и создавать современный информационный продукт; полученные навыки по решению актуальных практических задач в сфере защиты информации, управления предприятием. С этой целью в выпускной квалификационной работе требуется показать владение современными технологиями, а также умение систематизировать и использовать необходимую информацию.

В ходе подготовки магистерской работы 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 картографических и ГИС-технологий.

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.

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

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.

5.2. Требования к оформлению ВКР

Выпускная квалификационная работа должна соответствовать требованиям СТО СГУГиТ–011-2017. Стандарт организации 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 заимствований с использованием системы «Антиплагиат». ВКР магистрантов должна содержать не менее 75% оригинального текста. При не устранении плагиата после проверки работы или неспособности обучающегося в силу различных причин ликвидировать плагиат в установленные положением сроки, работа не допускается к защите, подлежит переработке.

5.3. Процедура защиты ВКР

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

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 выпускных квалификационных работ. 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 Государственной аттестационной комиссии;
- фонд оценочных средств для государственной итоговой аттестации;
- сведения о выпускниках, допущенных к защите;
- зачетные книжки;
- протоколы ГЭК.

Согласно этой процедуре, защита выпускной квалификационной работы 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. Доклад произносится свободно, своими словами, не зачитывая текст, а лишь опираясь на его положения. В выступлении следует обосновать актуальность темы, новизну рассматриваемых проблем и выводов, степень разработанности темы, кратко изложить основное содержание, выводы и предложения с убедительной аргументацией. 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 и рецензенту работы (при отсутствии кого-либо из них на защите отзыв и рецензия зачитываются).

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

Результат защиты определяется оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» и объявляется в тот же день после оформления в установленном порядке протоколов заседаний экзаменационной комиссии по защите выпускных квалификационных работ.

В тех случаях, когда защита ВКР признается неудовлетворительной, по решению ГЭК, обучающийся отчисляется из СГУГиТ и вместо диплома получает справку о прослушанных и сданных по учебному плану дисциплинах без присвоения квалификации.

ГЭК выносит решение, может ли обучающийся представить к повторной защите ту же работу с доработкой, определяемой комиссией, или же обязан выполнить работу по новой теме.

Решение ГЭК заносится в протокол. Протоколы заседаний подписываются председателем и секретарем государственной комиссии.

Результат защиты выпускной квалификационной работы и решение о присвоении квалификации выпускнику оформляются в зачетной книжке и заверяются подписями всех членов ГЭК, присутствовавших на заседании.

5.4. Методические рекомендации для оценки ВКР научным руководителем

Оформленная ВКР передается на отзыв научному руководителю. Обязанности научного руководителя ВКР состоят в следующем:

– содействие обучающемуся в выборе темы ВКР и разработке плана ее выполнения;

– оказание помощи в выборе методики проведения исследования и организации процесса написания работы;

– проведение консультаций по подбору нормативных актов, литературы, судебной практики, статистического и фактического материала;

– осуществление систематического контроля за полнотой и качеством подготавливаемых глав ВКР в соответствии с разработанным планом и своевременным представлением работы на кафедру;

– составление письменного отзыва о работе с оценкой качества ее выполнения в соответствии с предъявляемыми к ней требованиями;

– проведение подготовки и предварительной защиты ВКР с целью выявления готовности обучающегося к защите.

– принятие участия в защите ВКР и ответственность за качество представленной к защите ВКР.

После получения окончательного варианта ВКР научный руководитель составляет письменный отзыв. В отзыве научный руководитель дает анализ проведенной работе, отмечает личный вклад обучающегося в обоснование выводов и предложений, показывает особенности исследования. Заканчивается отзыв выводом о возможности или невозможности допуска данной работы к защите. После чего научный руководитель подписывает дипломную работу на титульном листе.

Объем отзыва должен составлять от одной до трех страниц машинописного текста.

5.5 Методические рекомендации для оценки ВКР рецензентом

ВКР направляется на рецензию специалисту, имеющему опыт по тематике работы. Рецензент отмечает актуальность темы, ее положительные стороны и недостатки и высказывает свое мнение о качестве данной работы. Объем рецензии должен составлять от одной до трех страниц машинописного текста. Подпись рецензента заверяется по месту работы в отделе кадров. Выпускник должен быть ознакомлен с рецензией не позднее, чем за пять дней до установленного срока защиты ВКР.

5.6. Методические рекомендации к докладу обучающегося по теме ВКР

Защита ВКР начинается с доклада обучающегося по теме работы. Продолжительность доклада составляет не более 15 минут. В докладе в первую очередь необходимо обосновать актуальность выбранной темы, далее нужно четко сформулировать цель проводимого исследования и рассказать о проделанной непосредственно автором работе, акцентировав внимание на полученных в ходе ее выполнения результатах. В докладе не следует излагать теоретические аспекты рассматриваемого вопроса, если они не являются дискуссионными. Обучающийся должен излагать основное содержание своей работы свободно, не читая письменный текст.

Рекомендуется в процессе доклада использовать заранее подготовленный наглядный графический материал (таблицы, схемы), иллюстрирующий основные положения работы. Объем иллюстративного материала не ограничивается.

5.7. Методические рекомендации для оценки ВКР членами Государственной экзаменационной комиссии

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 рецензента и присутствующих на защите.

Комиссия выставляет оценку за защиту ВКР на закрытом заседании. 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 его изучения. Исследование реализовано на основании достаточной источниковой базы, с применением актуальных методологических подходов. Работа имеет положительные отзыв научного руководителя. При ее защите выпускник показывает глубокие знания вопросов темы исследования, свободно оперирует данными исследования, вносит обоснованные предложения, эффективно использует новые информационные технологии при презентации своего доклада, убедительно иллюстрируя доклад диаграммами, схемами, таблицами, графиками, уверенно отвечает на поставленные вопросы.

– «хорошо» – выставляется за квалификационную работу, которая носит исследовательский характер, имеет грамотно изложенный теоретический раздел, в котором представлены достаточно подробный анализ и критический разбор концептуальных подходов и практической деятельности, последовательное изложение материала с соответствующими выводами, но с недостаточно обоснованными предложениями. Работа имеет положительные 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.

При положительной оценке Государственная экзаменационная комиссия принимает решение о присвоении обучающемуся квалификации (степени) с выдачей диплома об окончании СГУГиТ.

Организация и проведение государственной итоговой аттестации для инвалидов и лиц с ограниченными возможностями здоровья определяется локальным нормативным актом СГУГиТ.

6. ОЦЕНОЧНЫЕ СРЕДСТВА ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

6.1. Паспорт фонда оценочных средств по ГИА

Уровень сформированности компетенций выпускника определяется комплексно на основе следующих компонентов государственной итоговой аттестации: отзыва руководителя ВКР, качества выполненной работы, защиты ВКР, а также на основании результатов промежуточной аттестации.

Степень сформированности отдельных компетенций выпускника и уровень их освоения определяется в период государственной итоговой аттестации, в различных ее компонентах.

Таблица 5

Компетенции и компоненты их оценки в период государственной итоговой аттестации

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, 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
ОПК-2	способностью к самостоятельному обучению и применению новых методов исследования профессиональной деятельности	Отзыв руководителя
ПК-1	способностью анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты	Отзыв руководителя, рецензия
ПК-2	способностью разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности	Отзыв руководителя, 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	Отзыв руководителя, рецензия, текст

	становления современного информационного общества	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 исследований и технических разработок	Отзыв руководителя, рецензия, текст ВКР, защита ВКР
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. Типовые контрольные задания, или иные материалы, необходимые для оценки результатов освоения образовательной программы

Примерные темы выпускных квалификационных работ:

1. Разработка имитационной компьютерной модели для виртуальных исследований информационных систем.
2. Оценка эффективности средств защиты информации в государственных информационных системах.
3. Исследование методов мониторинга телекоммуникационной системы.
4. Разработка методики по проверке соответствия жизненного цикла программного обеспечения стандарту Secure SDLC
5. Разработка защищенного Web-интерфейса для управления техническими системами.
6. Оценка соответствия средств защиты информации на значимых объектах критической информационной инфраструктуры РФ.
7. Исследование методов обеспечения целостности информации.
8. Разработка имитационной компьютерной модели для виртуальных исследований информационных систем.
9. Защита информации в распределенной информационной системе предприятия ОПК.

10. Разработка подсистемы защиты информационного проекта предприятия от несанкционированного доступа.

11. Исследование надежности и безопасности функционирования фотоприемников систем контроля изображения.

12. Создание инфраструктуры обработки и защиты информации с использованием технологий виртуализации.

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

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

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

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

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

18. Разработка информационной системы для ведения реестра значимых объектов критической информационной инфраструктуры.

19. Голографическая защита информации. Передача оптического сигнала.

20. Голографическая защита информации. Регистрация оптического сигнала.

21. Организация и обеспечение информационной безопасности образовательного Интернета вещей.

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

23. Создание виртуальной лаборатории компьютерной безопасности.

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

25. Исследование современных информационных систем по поддержке управления приборостроительным предприятием в контексте обеспечения информационной безопасности.

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.
7 Что такое информационная безопасность?

6.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие формирование компетенций

6.3.1 Общие положения

Оценочные средства включают оценочные материалы, которые классифицируются по видам контроля:

– промежуточная аттестация, осуществляемая преподавателем после изучения теоретического материала дисциплины, прохождения производственных и преддипломной практики в форме практической подготовки;

– государственная итоговая аттестация, проводимая государственной экзаменационной комиссией.

Оценочные средства для государственной итоговой аттестации выпускников включают показатели и критерии оценки результата выполнения и защиты выпускной квалификационной

работы. Показатели оценки результата представляют собой формализованное описание оцениваемых основных параметров процесса или результата деятельности аттестуемого как составляющих общекультурных, общепрофессиональных и профессиональных компетенций ФГОС ВО. Показатели оценки результатов отражают комплексный результат деятельности.

Оценочные средства для государственной итоговой аттестации обеспечивают поэтапную и интегральную оценку компетенций выпускников.

Достижение показателей оценки результатов выполнения и защиты ВКР оценивается государственной экзаменационной комиссией, учитывая актуальность выбранной темы, практическую значимость, исполнительский уровень, а также методическое и информационное обеспечение. Критерии оценки результатов выполнения и защиты ВКР однозначны и логичны

Требования к содержанию, объему и структуре ВКР определяются СТО СГУГиТ–011-2017. Стандарт организации. Государственная итоговая аттестация выпускников СГУГиТ. Структура и правила оформления.

Разработанные задания на ВКР, основные показатели оценки результатов выполнения и защиты ВКР и критерии оценивания (оценочные средства ГИА) проходят предварительную экспертизу на соответствие требованиями ФГОС ВО и утверждаются на заседании выпускающей кафедры.

Оценка компетенций выпускников проводится государственной экзаменационной комиссией поэтапно с учетом оценок: общекультурных, общепрофессиональных и профессиональных компетенций выпускников, продемонстрированных при защите ВКР с учетом результатов промежуточной аттестации по учебным дисциплинам.

Критерии оценки выпускной квалификационной работы:

– понимает актуальность и значимость выбранной темы;
– осуществляет поиск и использует информацию, необходимую для эффективного выполнения профессиональных задач;
– устанавливает связь между теоретическими и практическими результатами и их соответствие с целями, задачами исследования;
– умеет структурировать знания, решать сложные практические задачи;
– обобщает результаты исследования, делает выводы;
– логично выстраивает защиту, аргументирует ответы на вопросы;
– защищает собственную профессиональную позицию;
– осуществляет самооценку деятельности и результатов (осознание и обобщение собственного уровня профессионального развития);
– предъявляет работу, оформленную в соответствии с основными требованиями нормоконтроля;
– сопровождает защиту качественной электронной презентацией, соответствующей структуре и содержанию ВКР.

6.3.2 Оценки уровня освоения компетенций на основе отзыва руководителя и рецензии

До защиты руководитель ВКР оформляет отзыв, в котором указываются личные качества обучающегося, его знания и способности, которые он проявил в ходе выполнения ВКР. Кроме того, руководитель должен оценить уровень сформированности у обучающегося каждой компетенции – повышенный, базовый или пороговый. Список компетенций, оцениваемых руководителем ВКР, представлен в таблице 6.

До защиты на ВКР должна быть получена рецензия, в которой отмечается актуальность темы исследования и дается общая характеристика ВКР. Кроме того, рецензент должен оценить уровень сформированности у обучающегося компетенции – повышенный, базовый или пороговый. Список компетенций, оцениваемых рецензентом, представлен в таблице 6.

Таблица 6

Уровни сформированности компетенций в процессе выполнения выпускной квалификационной работы

Оцениваемые компетенции	Показатели, оцениваемые руководителем	5	4	3
ОК-1 - способностью к абстрактному мышлению, анализу, синтезу	степень способности	повышенный	базовый	пороговый
ОК-2 - способностью самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения	степень способности	повышенный	базовый	пороговый
ОПК-1 - способностью к коммуникации в устной и письменной формах на государственном и одном из иностранных языков для решения задач профессиональной деятельности	степень готовности	повышенный	базовый	пороговый
ОПК-2 - способностью к самостоятельному обучению и применению новых методов исследования профессиональной деятельности	степень готовности	повышенный	базовый	пороговый
ПК-1 - способностью анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты	степень готовности	повышенный	базовый	пороговый
ПК-2 - способностью разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности	степень готовности	повышенный	базовый	пороговый
ПК-3 - способностью проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов	степень способности	повышенный	базовый	пороговый
ПК-4 - способностью разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности	степень способности	повышенный	базовый	пороговый

ПК-5 - способностью анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества	степень способности	повышенный	базовый	пороговый
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	степень способности	повышенный	базовый	пороговый
ПК-7 - способностью проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента	степень способности	повышенный	базовый	пороговый
ПК-8 - способностью обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи	степень способности	повышенный	базовый	пороговый
ПК-12 - способностью организовать выполнение работ, управлять коллективом исполнителей и принимать управленческие решения	степень способности и готовности	повышенный	базовый	пороговый
ПК-13 - способностью организовать управление информационной безопасностью	степень способности	повышенный	базовый	пороговый
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	степень способности	повышенный	базовый	пороговый
ПК-15 - способностью организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности	степень способности	повышенный	базовый	пороговый
ПК-16 - способностью разрабатывать проекты организационно-	степень способности	повышенный	базовый	пороговый

распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности				
Итоговая оценка руководителя*				

* Оценка «отлично» выставляется, если по всем критериям получены оценки «отлично», не более одного критерия «хорошо».

Оценка «хорошо» выставляется, если по всем критериям получены оценки «хорошо» и «отлично» не более одного критерия «удовлетворительно».

Оценка «удовлетворительно» выставляется, если по всем критериям оценки положительные, не более одного критерия «неудовлетворительно».

Оценка «неудовлетворительно», если получено по критериям более одной неудовлетворительной оценки.

6.3.3 Оценки уровня освоения компетенций на основе содержания ВКР и процедуры Защиты

На защите члены экзаменационной комиссии оценивают выполненную обучающимся ВКР по содержательной части в соответствии с критериями, представленными в таблице. При этом учитывается качество доклада и иллюстрационного материала.

Таблица 7

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

Оцениваемые компетенции	Показатели оценки ВКР	5	4	3
ОК-2, ОПК-2, ПК-1, ПК-2, ПК-4, ПК-6, ПК-7, ПК-14, ПК-15	Уровень актуальности и обоснования выбора темы	повышенный	базовый	пороговый
	Уровень завершенности работы	повышенный	базовый	пороговый
	Уровень объема и глубины знаний по теме	повышенный	базовый	пороговый
	Уровень достоверности и обоснованности полученных результатов и выводов	повышенный	базовый	пороговый
	Уровень наличия материала, подготовленного к практическому использованию	повышенный	базовый	пороговый
	Уровень применения новых подходов	повышенный	базовый	пороговый
ОПК-1, ПК-8, ПК-12, ПК-16	Уровень качества доклада (полнота представления работы, эрудиция, использование междисциплинарных связей убежденность автора)	повышенный	базовый	пороговый
	Уровень качества оформления ВКР и демонстрационных материалов	повышенный	базовый	пороговый
	Уровень коммуникаций: куль-	повышенный	базовый	пороговый

	тура речи, манера общения, умение использовать наглядные пособия, способность заинтересовать аудиторию			
ПК-3, ПК-5, ПК-13	Уровень ответов на вопросы: полнота, аргументированность, убежденность, умение использовать ответы на вопросы для более полного раскрытия содержания проведенной работы	повышенный	базовый	пороговый
Итоговая оценка членов ГЭК*				

* Оценка «отлично» выставляется, если по всем критериям получены оценки «отлично», не более одного критерия «хорошо». Оценка «хорошо» выставляется, если по всем критериям получены оценки «хорошо» и «отлично» не более одного критерия «удовлетворительно».

Оценка «удовлетворительно» выставляется, если по всем критериям оценки положительные, не более одного критерия «неудовлетворительно». Оценка «неудовлетворительно», если получено по критериям более одной неудовлетворительной оценки.

Итоговая оценка за выполнение и защиту выпускной квалификационной работы в ходе проведения итоговой государственной аттестации выставляется обучающемуся с учетом всех полученных оценок по вышеуказанным критериям и показателям:

– отзыв руководителя ВКР;

– рецензия на ВКР;

– оценка членов ГЭК по содержанию ВКР, качеству ее защиты, оформления и презентации.

Общая оценка ГЭК определяется как средняя арифметическая величина из оценок членов ГЭК.

Итоговая оценка выставляется исходя из следующих условии: «отлично» выставляется, если по всем критериям получены оценки «отлично», и не более одного критерия «хорошо»; «хорошо» выставляется, если по всем критериям получены оценки «хорошо» и «отлично» и не более одного критерия «удовлетворительно»; «удовлетворительно» выставляется, если по всем критериям оценки положительные, и не более одного критерия «неудовлетворительно»; «неудовлетворительно» выставляется, если получено по критериям более одной неудовлетворительной оценки.

Итоговая оценка по ГИА выпускника может быть увеличена на 1 балл из учета уровня освоения им ОП по результатам оценок промежуточной аттестации, полученных в период обучения.

Подача и рассмотрение апелляционных заявлений по результатам государственных аттестационных испытаний регулируется локальным нормативным актом СГУГиТ.

7. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ГИА

7.1 Основная литература:

№ п/п	*Библиографическое описание*	*Количество экземпляров в библиотеке СГУГиТ*
1.	Алексеев, Е. Б. Проектирование и техническая эксплуатация цифровых телекоммуникационных систем и сетей [Электронный ресурс] : учеб. по-	Электронный ресурс

	собие / Е. Б. Алексеев, В. Н. Гордиенко, В. В. Крухмалев [и др.] ; под редакцией В. Н. Гордиенко, М. С. Тверецкого. – 2-е изд., испр. – М. : Горячая линия-Телеком, 2017. – 392 с. – Режим доступа: https://e.lanbook.com/book/111002 – Загл. с экрана.	
2.	Амос, Г. MATLAB. Теория и практика [Электронный ресурс] / Г. Амос ; пер. с англ. Н. К. Смоленцев. – М. : ДМК Пресс, 2016. – 416 с. – Режим доступа: https://e.lanbook.com/book/82814 – Загл. с экрана.	Электронный ресурс
3.	Английский язык. English for Discussion (Английский язык для обсуждения) [Электронный ресурс] : метод. указания / Е. В. Душинина ; СГГА. – Новосибирск : СГГА, 2014. – 41, [1] с. – Режим доступа: http://lib.ssga.ru – Загл. с экрана.	Электронный ресурс
4.	Английский язык [Электронный ресурс] : практикум / С. С. Жданов, Л. М. Никулина; СГГА. – Новосибирск : СГГА, 2014. – 107, [1] с. – Режим доступа: http://lib.ssga.ru – Загл. с экрана.	Электронный ресурс
5.	Барабанов, А. В. Семь безопасных информационных технологий [Электронный ресурс] : учебник / А. В. Барабанов, А. В. Дорофеев, А. С. Марков, В. Л. Цирлов ; под ред. А. С. Маркова. – М. : ДМК Пресс, 2017. – 224 с. – Режим доступа: https://e.lanbook.com/book/97352 – Загл. с экрана.	Электронный ресурс
6.	Баранова, Е. К. Информационная безопасность и защита информации [Электронный ресурс] : учеб. пособие / Е. К. Баранова, А.В. Бабаш. – 4-е изд., перераб. и доп. – М. : ИЦ РИОР, НИЦ ИНФРА-М, 2018. – 336 с. – Режим доступа: http://znanium.com/bookread2.php?book=957144 – Загл. с экрана.	Электронный ресурс
7.	Баранова Е. К. Актуальные вопросы защиты информации [Электронный ресурс] : монография / Е. К. Баранова, А. В. Бабаш. – М. : РИОР: ИНФРА-М, 2018. – 111 с. – Режим доступа: http://znanium.com/bookread2.php?book=979073 – Загл. с экрана.	Электронный ресурс
8.	Боуш, Г. Д. Методология научных исследований (в курсовых и выпускных квалификационных работах) [Электронный ресурс] : учебник / Г. Д. Боуш, В. И. Разумов. – М. : ИНФРА-М, 2019. – 210 с. – Режим доступа: http://znanium.com/catalog/product/991912 – Загл. с экрана.	Электронный ресурс
9.	Вводно-коррективный курс по английскому языку [Электронный ресурс] : практикум / А. С. Бочарова [и др.] ; СГУГиТ. – Новосибирск : СГУГиТ, 2016. – 70, [1] с. – Режим доступа: http://lib.ssga.ru – Загл. с экрана.	Электронный ресурс
10.	Водяхо, А. И. Архитектурные решения информационных систем [Электронный ресурс] : учебник / А. И. Водяхо, Л. С. Выговский, В. А. Дубенецкий, В. В. Цехановский. – СПб. : Лань, 2017. – 356 с. – Режим доступа: https://e.lanbook.com/book/96850 – Загл. с экрана.	Электронный ресурс
11.	Волкова, В. Н. Системный анализ информационных комплексов [Электронный ресурс] : учеб. пособие / В. Н. Волкова. – СПб. : Лань, 2016. – 336 с. – Режим доступа: https://e.lanbook.com/book/75506 – Загл. с экрана.	Электронный ресурс
12.	Ворона, В. А. Комплексные (интегрированные) системы обеспечения безопасности. Серия «Обеспечение безопасности объектов»; Выпуск 7 [Электронный ресурс] / В. А. Ворона, В. А. Тихонов. – М. : Горячая линия-Телеком, 2013. – 160 с. – Режим доступа: https://e.lanbook.com/book/5136 – Загл. с экрана.	Электронный ресурс
13.	Ворона, В. А. Системы контроля и условного доступа. Серия «Обеспечение безопасности объектов»; Выпуск 2 [Электронный ресурс] / В. А. Ворона, В. А. Тихонов. – М. : Горячая линия-Телеком, 2013. – 272 с. – Режим доступа: https://e.lanbook.com/book/5135 – Загл. с экрана.	Электронный ресурс

14.	Гвоздева, Т. В. Проектирование информационных систем. Стандартизация [Электронный 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
15.	Гилязова Р. Н. Информационная безопасность. Лабораторный практикум [Электронный ресурс] : учеб. пособие / Р. Н. Гилязова. – М. : Издательство «Лань», 2020. – 44 с. – Режим доступа: https://e.lanbook.com/book/93278?category=1545 – Загл. с экрана.	Электронный ресурс
16.	Глория, Б. Г. Обработка изображений с помощью Open CV [Электронный ресурс] / Б. Г. Глория, Д. С. Оскар, Л. Э. Хосе, С. Г. Исмаэль. – М. : ДМК Пресс, 2016. – 210 с. – Режим доступа: http://e.lanbook.com/book/90116 – Загл. с экрана.	Электронный ресурс
17.	Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками [Электронный ресурс] : учеб. пособие / П. Н. Девянин. – М. : Горячая линия-Телеком, 2013. – 338 с. – Режим доступа: https://e.lanbook.com/book/63235. – Загл. с экрана.	Электронный ресурс
18.	Зайцев, А. П. Технические средства и методы защиты информации [Электронный ресурс] : учебник / А. П. Зайцев, Р. В. Мещеряков, А. А. Шелупанов. – 7-е изд., испр. – М. : Горячая линия-Телеком, 2018. – 442 с. – Режим доступа: https://e.lanbook.com/book/111057 – Загл. с экрана.	Электронный ресурс
19.	Золотухина Е. Б. Управление жизненным циклом информационных систем (продвинутый курс) [Электронный ресурс] / Е. Б. Золотухина, С. А. Красникова, А.С. Вишня. – М. : КУРС, НИЦ ИНФРА-М, 2017. – 119 с. – Режим доступа: http://znanium.com/bookread2.php?book=767219 – Загл. с экрана.	Электронный ресурс
20.	Информационные технологии в оптотехнике и системах защиты информации [Текст] : учеб. пособие / Е. В. Грицкевич, П. А. Звягинцева ; СГУГиТ. – Новосибирск : СГУГиТ, 2016. – 47. [1] с.	80
21.	Итоговая государственная аттестация выпускников СГУГиТ. Структура и правила оформления [Текст] : СТО СГУГиТ 011-2017 / СТУГиТ. – Взамен СТО СГГА-011-2015 : Введ. С 2015-03-20. – Новосибирск : СГУГиТ, 2017. 67, [1] с.	56
22.	Ищуков, Е. А. Криптографические протоколы и стандарты [Электронный ресурс] : учеб. пособие / Е.А. Ищуков, Е.А. Лобова. – Таганрог : Южный федеральный университет, 2016. – 80 с. – Режим доступа: http://znanium.com/bookread2.php?book=991903 – Загл. с экрана.	Электронный ресурс
23.	Коллинз, М. Защита сетей. Подход на основе анализа данных [Электронный ресурс] / М. Коллинз. – М. : ДМК Пресс, 2020. – 308 с. – Режим доступа: https://e.lanbook.com/book/131682?category=1545 – Загл. с экрана.	Электронный ресурс
24.	Космин, В. В. Основы научных исследований (Общий курс) [Электронный ресурс] : учеб. пособие / В. В. Космин. – 3-е изд., перераб. и доп. – М. : ИЦ РИОР, НИЦ ИНФРА-М, 2016. – 227 с. – Режим доступа: http://znanium.com/catalog/product/518301 – Загл. с экрана.	Электронный ресурс
25.	Костюк, А. В. Информационные технологии. Базовый курс [Электронный ресурс] : учебник / А. В. Костюк, С. А. Бобонец, А. В. Флегонтов, А. К. Черных. – 2-е изд., стер. – СПб. : Лань, 2019. – 604 с. – Режим доступа: https://e.lanbook.com/book/114686 – Загл. с экрана.	Электронный ресурс
26.	Кравчук, И. Л. Риск негативных событий, обусловленный нарушениями требований безопасности, и способ его снижения. Отдельная статья: Горный информационно-аналитический бюллетень (научно-технический журнал) [Электронный ресурс] / И. Л. Кравчук, В. Ю. Гришин, А. В. Смолин. – М. : Горная книга, 2015. – 20 с. – Режим доступа: https://e.lanbook.com/book/101705 – Загл. с экрана.	Электронный ресурс

27.	Крук, Б. И. Телекоммуникационные системы и сети [Электронный ресурс] : учеб. пособие : в 3 томах / Б. И. Крук, В. Н. Попантонопуло, В. П. Шувалов ; под редакцией В. П. Шувалова. – 4-е изд., испр. и доп. – М. : Горячая линия-Телеком, [б. г.]. – Том 1 : Современные технологии – 2018. – 620 с. – Режим доступа: https://e.lanbook.com/book/111070 – Загл. с экрана.	Электронный ресурс
28.	Крюкова, Н. П. Документирование управленческой деятельности [Электронный ресурс] : учеб. пособие / Н. П. Крюкова. – М. : ИНФРА-М, 2014. – 268 с. – Режим доступа: http://znanium.com/bookread2.php?book=432033 – Загл. с экрана.	Электронный ресурс
29.	Кэлер, А. Изучаем Open CV 3. Разработка программ компьютерного зрения на C++ с применением библиотеки Open CV [Электронный ресурс] / А. Кэлер, Г. Брэдски ; пер. с анг. А. А. Слинкина. – М. : ДМК Пресс, 2017. – 826 с. – Режим доступа: https://e.lanbook.com/book/108126 – Загл. с экрана.	Электронный ресурс
30.	Латыев, С. М. Конструирование точных (оптических) приборов [Электронный ресурс] : учеб. пособие / С. М. Латыев. – СПб. : Лань, 2015. – 560 с. – Режим доступа: https://e.lanbook.com/book/60655 – Загл. с экрана.	Электронный ресурс
31.	Левушкина, С. В. Кадровая политика и кадровый аудит организаций [Электронный ресурс] : учеб. пособие / сост. С. В. Левушкина. – Ставрополь : Ставропольский гос. аграрный ун-т, 2014. – 168 с. – Режим доступа: http://znanium.com/catalog.php?bookinfo=514173 – Загл. с экрана.	Электронный ресурс
32.	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.	Электронный ресурс
33.	Менеджмент риска информационной безопасности [Электронный ресурс] : учеб. пособие / Г. Е. Веселов, Е. С Абрамов, А. К. Шилов. – Таганрог : Южный федеральный университет, 2016. – 107 с. – Режим доступа: http://znanium.com/catalog/product/997108 – Загл. с экрана.	Электронный ресурс
34.	Милославская, Н. Г. Управление инцидентами информационной безопасности и непрерывностью бизнеса. Серия «Вопросы управления информационной безопасностью". Выпуск 3 [Электронный ресурс] : учеб. пособие / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. – М. : Горячая линия-Телеком, 2013. – 170 с. – Режим доступа: https://e.lanbook.com/book/5180 – Загл. с экрана.	Электронный ресурс
35.	Монаппа, К. А. Анализ вредоносных программ [Электронный ресурс] : учеб. пособие / К. А. Монаппа. – М. : ДМК Пресс, 2019. – 452 с. – Режим доступа: https://e.lanbook.com/book/123709?category=1545 – Загл. с экрана.	Электронный ресурс
36.	Новиков, С. Н. Методология защиты пользовательской информации на основе технологий сетевого уровня мультисервисных сетей связи [Электронный ресурс] / С. Н. Новиков. – М. : Горячая линия-Телеком, 2018. – 128 с. – Режим доступа: https://e.lanbook.com/book/119836 – Загл. с экрана.	Электронный ресурс
37.	Овчаров, А. О. Методология научного исследования [Электронный ресурс] : учебник / А. О. Овчаров, Т. Н. Овчарова. – М. : НИЦ ИНФРА-М, 2020. – 304 с. – Режим доступа: https://znanium.com/read?id=353899 – Загл. с экрана.	Электронный ресурс
38.	Оптика [Текст] : учеб. пособие / В. С. Акиньшин [и др.]; ред. С. К. Стафеев. – 2-ое изд., перераб. – СПб. : Лань, 2015. – 232 с.	25
39.	Остапенко, Г. Ф. Управление интеллектуальной собственностью [Электронный ресурс] : учеб. пособие для магистров / Г. Ф. Остапенко, А. Д. Остапенко. – М. : Дашков и К, 2016. – 160 с. – Режим доступа: http://znanium.com/bookread2.php?book=937305 – Загл. с экрана.	Электронный ресурс

40.	Программно-аппаратная защита информации [Электронный ресурс] : учеб. пособие / П. Б. Хорев. – 2-е изд., испр. и доп. – М. : Форум: НИЦ ИНФРА-М, 2015. – 352 с. – Режим доступа: http://znanium.com/bookread2.php?book=489084 – Загл. с экрана.	Электронный ресурс
41.	Прохорова, О. В. Информационная безопасность и защита информации [Электронный ресурс] : учебник / О .В. Прохорова. – М. : Издательство «Лань», 2020. – 124 с. – Режим доступа: https://e.lanbook.com/book/133924?category=1545 – Загл. с экрана.	Электронный ресурс
42.	Радовель В. А. Английский язык для технических вузов [Электронный ресурс] : учеб. пособие / В. А. Радовель. – М. : РИОР: ИНФРА-М, 2017. – 284 с. – Режим доступа: http://znanium.com/bookread2.php?book=794676 – Загл. с экрана.	Электронный ресурс
43.	Симонов, С. В. Управление информационными рисками. Экономически оправданная безопасность [Электронный ресурс] : учеб. пособие / С. В. Симонов, С. А. Петренко. – 2-е изд., (эл.). – М. : ДМК Пресс, 2018. – 396 с. – Режим доступа: http://znanium.com/bookread2.php?book=983162 – Загл. с экрана.	Электронный ресурс
44.	Теория организации. Структура и основы деятельности организаций [Текст] : учеб. пособие / О. В. Грицкевич, Л. А. Савельева ; СГУГиТ. – Новосибирск : СГУГиТ, 2017. – 132, [1] с.	30
45.	Управление проектами: фундаментальный курс [Электронный ресурс] : учебник / А. В. Алешин, В. М. Аньшин, К. А. Багратиони и др. ; под ред. В. М. Аньшина, О. Н. Ильиной ; Нац. исслед. ун-т «Высшая школа экономики». – М. : Изд. дом Высшей школы экономики, 2013 – 620 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=227270 – Загл. с экрана.	Электронный ресурс
46.	Управление проектами [Электронный ресурс] : учеб. пособие / Ю. И. Попов, О. В. Яковенко. – М. : ИНФРА-М, 2019. – 208 с. – Режим доступа: http://znanium.com/catalog/product/983557 – Загл. с экрана.	Электронный ресурс
47.	Управление проектами (проектный менеджмент) [Электронный ресурс] : учеб. пособие / Г. А. Поташева. – М. : ИНФРА-М, 2018. – 224 с. – Режим доступа: http://znanium.com/catalog/product/930921 – Загл. с экрана.	Электронный ресурс
48.	Управление проектами [Электронный ресурс] : учебник / под ред. Н. М. Филимоновой, Н. В. Моргуновой, Н. В. Родионовой. – М. : ИНФРА-М, 2018. – 349 с. – Режим доступа: http://znanium.com/catalog/product/918075 – Загл. с экрана.	Электронный ресурс
49.	Шаньгин, В. Ф. Информационная безопасность [Электронный ресурс] : учеб. пособие / В. Ф. Шаньгин. – М. : ДМК Пресс, 2014. – 702 с. – Режим доступа: https://e.lanbook.com/book/50578. – Загл. с экрана.	Электронный ресурс

7.2 Дополнительная литература

№ п/п	*Библиографическое описание*
1.	Авдошин, С. М. Информатизация бизнеса. Управление рисками [Электронный ресурс] : учебник / С. М. Авдошин, Е. Ю. Песоцкая. – М. : ДМК Пресс, 2011. – 176 с. – Режим доступа: https://e.lanbook.com/book/302 – Загл. с экрана.
2.	Афанасьев, А. А. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам [Электронный ресурс] / А. А. Афанасьев, Л. Т. Веденьев, А. А. Воронцов, Э. Р. Газизова. – М. : Горячая линия-Телеком, 2012. – 550 с. – Режим доступа: http://e.lanbook.com/book/5114 – Загл. с экрана.
3.	Бирюков, А. А. Информационная безопасность: защита и нападение [Электронный ре-

	сурс] : учебник / А. А. Бирюков. – М. : ДМК Пресс, 2012. – 474 с. – Режим доступа: https://e.lanbook.com/book/39990 – Загл. с экрана.
4.	Благодаров, А. В. Алгоритмы категорирования персональных данных для систем автоматизированного проектирования баз данных информационных систем [Электронный ресурс] / А. В. Благодаров, В. С. Зияутдинов, П. А. Корнев, В. Н. Малыш. – М. : Горячая линия-Телеком, 2013. – 116 с. – Режим доступа: https://e.lanbook.com/book/11827 – Загл. с экрана.
5.	Бутиков, Е. И. Оптика [Электронный ресурс] : учеб. пособие / Е. И. Бутиков. – 3-е изд., доп. – СПб. : Лань, 2012. – 607 с.
6.	Ворона, В. А. Инженерно-техническая и пожарная защита объектов. Серия «Обеспечение безопасности объектов»; Выпуск 4 [Электронный ресурс] / В. А. Ворона, В. А. Тихонов. – – М. : Горячая линия-Телеком, 2012. – 512 с. – Режим доступа: http://e.lanbook.com/book/5139 – Загл. с экрана.
7.	Ворона, В. А. Концептуальные основы создания и применения системы защиты объектов. Серия «Обеспечение безопасности объектов»; Выпуск 1 [Электронный ресурс] / В. А. Ворона, В. А. Тихонов. – М. : Горячая линия-Телеком, 2012. – 184 с. – Режим доступа: http://e.lanbook.com/book/5137 – Загл. с экрана.
8.	Горбунов, В. А. Математические методы в теории защиты информации [Электронный ресурс] / В. А. Горбунов. – М. : Горная книга, 2004. – 82 с. – Режим доступа: https://e.lanbook.com/book/3490 – Загл. с экрана.
9.	Грибунин, В. Г. Комплексная система защиты информации на предприятии [Текст] : учеб. пособие для вузов / В. Г. Грибунин, В. В. Чудовский . – М. : Академия, 2009. – 411 с.
10.	Грушо, А. А. Теоретические основы компьютерной безопасности [Текст] : учеб. пособие для вузов (рек.) / А. А. Грушо, Э. А. Применко, Е. Е. Тимонина. – М. : Академия, 2009. – 272 с.
11.	Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. [Электронный ресурс] / П. Н. Девянин. – М. : Горячая линия-Телеком, 2012. – 320 с. – Режим доступа: http://e.lanbook.com/book/5150 – Загл. с экрана.
12.	Жукова, М. Н. Управление информационной безопасностью. Ч. 2. Управление инцидентами информационной безопасности [Электронный ресурс] : учеб. пособие / М. Н. Жукова, В. Г. Жуков, В. В. Золотарев. – Красноярск : Сиб. гос. аэрокосмич. ун-т, 2012. – 100 с – Режим доступа: http://znanium.com/bookread2.php?book=463061 – Загл. с экрана.
13.	Зайцев, А. П. Технические средства и методы защиты информации [Электронный ресурс] / А. П. Зайцев, А. А. Шелупанов, Р. В. Мещеряков. – М : Горячая линия-Телеком, 2012. – 442 с. – Режим доступа: http://e.lanbook.com/book/5155 – Загл. с экрана.
14.	Защита информации [Электронный ресурс] : учеб. пособие / А. П. Жук, Е. П. Жук, О. М. Лепешкин, А. И. Тимошкин. – 2-е изд. – М. : РИОР: ИНФРА-М, 2018. – 392 с. – Режим доступа: http://znanium.com/bookread2.php?book=937469 – Загл. с экрана.
15.	Ишанин, Г. Г. Приемники оптического излучения [Текст] : учебник / Г. Г. Ишанин, В. П. Челибанов; ред. В. В. Коротаев. – СПб. : Лань, 2014. – 303, [1] с.
16.	Коваленко, Ю. И. Правовой режим лицензирования и сертификации в сфере информационной безопасности [Электронный ресурс] / Ю. И. Коваленко. – М. : Горячая линия-Телеком, 2012. – 140 с. – Режим доступа: http://e.lanbook.com/book/5163 – Загл. с экрана.
17.	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.
18.	Магазинникова, А. Л. Основы цифровой обработки сигналов [Электронный ресурс] : учеб. пособие / А. Л. Магазинникова. – СПб. : Лань, 2016. – 132 с. – Режим доступа: https://e.lanbook.com/book/76274 – Загл. с экрана.

19.	Малюк, А. А. Теория защиты информации [Электронный ресурс] / А. А. Малюк. – М. : Горячая линия-Телеком, 2012. – 184 с. – Режим доступа: http://e.lanbook.com/book/5170. – Загл. с экрана.
20.	Малюк, А. А. Теория защиты информации [Электронный ресурс] / А. А. Малюк. – М. : Горячая линия-Телеком, 2015. – 184 с. – Режим доступа: https://e.lanbook.com/book/111077 – Загл. с экрана.
21.	Малюк, А. А. Этика в сфере информационных технологий [Электронный ресурс] / А. А. Малюк, О. Ю. Полянская, И. Ю. Алексеева. – М. : Горячая линия-Телеком, 2011. – 288 с. – Режим доступа: http://e.lanbook.com/book/5172 – Загл. с экрана.
22.	Манойло, А. В. Государственная информационная политика в условиях информационно-психологической войны [Электронный ресурс] / А. В. Манойло, А. И. Петренко, Д. Б. Фролов. – 2-е изд., стер. – М. : Горячая линия-Телеком, 2017. – 542 с. – Режим доступа: https://e.lanbook.com/book/111080 – Загл. с экрана.
23.	Масалков, А. С. Особенности киберпреступлений: инструменты нападения и защиты информации [Электронный ресурс] / А. С. Масалков. – М. : ДМК Пресс, 2018. – 226 с. – Режим доступа: https://e.lanbook.com/book/105842 – Загл. с экрана.
24.	Мельников, В. П. Информационная безопасность и защита информации [Текст] : учеб. пособие для вузов, допущено УМО / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; ред. С. А. Клейменов. – 5-е изд., стереотип. – М. : Академия, 2011. – 330, [6] с.
25.	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.
26.	Милославская, Н. Г. Проверка и оценка деятельности по управлению информационной безопасностью. Серия «Вопросы управ ления 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.
27.	Нестеренко, А. В. Международные стандарты аудита [Электронный ресурс] : учеб. пособие / А. В. Нестеренко, Т. Ю. Бездольная. – 5-е изд., перераб. и доп. – Ставрополь : АГРУС, 2013. – 156 с. – Режим доступа: http://znanium.com/catalog.php?bookinfo=514247 – Загл. с экрана.
28.	Нестеров, С. А. Основы информационной безопасности [Электронный ресурс] : учеб. пособие / С. А. Нестеров. – 5-е изд., стер. – СПб. : Лань, 2019. – 324 с. – Режим доступа: https://e.lanbook.com/book/114688 – Загл. с экрана.
29.	Никифоров, С. Н. Методы защиты информации. Защищенные сети [Электронный ресурс] : учеб. пособие / С. Н. Никифоров. – СПб. : Лань, 2018. – 96 с. – Режим доступа: https://e.lanbook.com/book/110935 – Загл. с экрана.
30.	Организация и проведение научно-педагогической и научно-исследовательской практики магистрантов [Текст] : метод. указания / В. А. Павленко, С. В. Середович, А. В. Веселков ; СГГА. – Новосибирск : СГГА, 2014. – 15, [1] с.
31.	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.
32.	Остроух, А. В. Интеллектуальные информационные системы и технологии [Электронный ресурс] : монография / А. В. Остроух, А. Б. Николаев. – СПб. : Лань, 2019. – 308 с. – Режим доступа: https://e.lanbook.com/book/115518 – Загл. с экрана.
33.	Петренко, С. А. Аудит безопасности Intranet [Электронный ресурс] : учеб. пособие / С. А. Петренко, А. А. Петренко. – М. : ДМК Пресс, 2010. – 386 с. – Режим доступа: https://e.lanbook.com/book/1113 – Загл. с экрана.

34.	Порфирьев, Л. Ф. Основы теории преобразования сигналов в оптико-электронных системах [Электронный ресурс] : учебник / Л. Ф. Порфирьев. – СПб. : Лань, 2013. – 400 с. – Режим доступа: https://e.lanbook.com/book/12942. – Загл. с экрана.
35.	Правовая защита информации [Электронный ресурс] : учеб. пособие / А. И. Маркеев ; СГГА. – Новосибирск : СГГА, 2011. – 180 с. – Режим доступа: http://lib.sgugit.ru – Загл. с экрана.
36.	Региональная и национальная безопасность [Электронный ресурс] : учеб. пособие / А. Б. Логунов. – 2-е изд., перераб. и доп. – М. : Вузовский учебник: ИНФРА-М, 2014. – 448 с. – Режим доступа: http://znanium.com/bookread2.php?book=406872 – Загл. с экрана.
37.	Серебрякова, Т. Ю. Риски организации и внутренний экономический контроль [Электронный ресурс] : монография / Т. Ю. Серебрякова. – М. : ИНФРА-М, 2019. – 111 с. – Режим доступа: http://znanium.com/catalog/product/1031520 – Загл. с экрана.
38.	Родичев, Ю. А. Информационная безопасность: нормативно-правовые аспекты [Текст] : учеб. пособие для вузов (доп.) / Ю. А. Родичев. – СПб. : ПИТЕР, 2008. – 272 с.
39.	Рудинский, И. Д. Технология проектирования автоматизированных систем обработки информации и управления [Электронный ресурс] / И. Д. Рудинский, – М. : Горячая линия-Телеком, 2011. – 304 с. – Режим доступа: http://e.lanbook.com/book/5191 – Загл. с экрана.
40.	Сабанов, А. Г. Защита персональных данных в организациях здравоохранения [Электронный ресурс] / А. Г. Сабанов, В. Д. Зыков, Р. В. Мещеряков. – М. : Горячая линия-Телеком, 2012. – 206 с. – Режим доступа: http://e.lanbook.com/book/5194 – Загл. с экрана.
41.	Семенов, А. Б. Проектирование и расчет структурированных кабельных систем и их компонентов [Электронный ресурс] / А. Б. Семенов. – М. : ДМК Пресс, 2010. – 416 с. – Режим доступа: https://e.lanbook.com/book/1141 – Загл. с экрана.
42.	Скрипкин, К. Г. Экономическая эффективность информационных систем в России [Электронный ресурс] : монография. – М. : МАКС Пресс, 2014. – 156 с. – Режим доступа: https://e.lanbook.com/book/104884 – Загл. с экрана.
43.	Теоретические основы управления в организациях [Электронный ресурс] : учеб. пособие / В. П. Балан, А. В. Душкин, В. И. Новосельцев, В. И. Сумин ; под ред. В. И. Новосельцев. – М. : Горячая линия-Телеком, 2016. – 244 с. – Режим доступа: https://e.lanbook.com/book/107634 – Загл. с экрана.
44.	Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях [Электронный ресурс] / В. Ф. Шаньгин. – М. : ДМК Пресс, 2012. – 592 с. – Режим доступа: http://e.lanbook.com/book/3032 – Загл. с экрана.
45.	Фостер, Д. Защита от взлома: сокеты, эксплойты, shell-код [Электронный ресурс] / Д. Фостер. – М. : ДМК Пресс, 2008. – 784 с. – Режим доступа: https://e.lanbook.com/book/1117 – Загл. с экрана.

7.3 Ресурсы сети «Интернет»

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. – 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);

– компьютерная справочная правовая система «Консультант-Плюс». – Режим доступа: http://www.consultant.ru/ (доступ с любого компьютера, подключенного к интернету);

– электронная информационно-образовательная среда СГУГиТ).