Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Уральский государственный университет путей сообщения»

Кафедра *«Информационные технологии и защита информации»*

СОГЛАСОВАНО
председатель ГЭК по образовательной
программе ОП ВО
«Информационная безопасность»

_____ /А.А. Захаров

«30» декабря 2016 г

УТВЕРЖДАЮ
Проректор по учебной работе
и связям с производством

_____ / Е. А. Малыгин

«30» декабря 2016 г

ПРОГРАММА
ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки

10.03.01 «Информационная безопасность»
(код и наименование направления подготовки (специальности))

«Организация и технология защиты информации (на транспорте)»
(наименование направленности (профиля) образовательной программы (специализации))

Квалификация
бакалавр

Форма обучения
очная

Екатеринбург
2016

Оглавление

1 Общие положения

Целью государственной итоговой аттестации является установление соответствия результатов освоения обучающимися образовательной программы 10.03.01 «Информационная безопасность», разработанной в Уральском государственном университете путей сообщения, требованиям Федерального государственного образовательного стандарта высшего образования (ФГОС ВО), и оценка уровня подготовленности выпускника к самостоятельной профессиональной деятельности.

Лицам, успешно прошедшим государственную итоговую аттестацию присваивается квалификация бакалавр.

Процедура организации и проведения государственной итоговой аттестации обучающихся, завершающей освоение имеющих государственную аккредитацию образовательных программ, включая формы государственных аттестационных испытаний, требования, предъявляемые к лицам, привлекаемым к проведению государственной итоговой аттестации, порядок подачи и рассмотрения апелляций, изменения и (или) аннулирования результатов государственной итоговой аттестации, а также особенности проведения государственной итоговой аттестации для обучающихся из числа лиц с ограниченными возможностями здоровья в университетском комплексе Уральского государственного университета путей сообщения (далее УрГУПС или университет) единые по университету и закреплены в Положении ПЛ 2.3.23 – 2017 «Порядок проведения государственной итоговой аттестации по образовательным программам высшего образования – по программам бакалавриата, программам специалитета и программам магистратуры».

2 Структура государственной итоговой аттестации и ее трудоемкость

Государственная итоговая аттестация по данной образовательной программе проводится в форме защиты выпускной квалификационной работы.

Государственная итоговая аттестация проводится в 8 семестре согласно календарного учебного графика. Общая трудоемкость составляет 6 зачетных единиц (216 часов).

3 Перечень планируемых результатов освоения образовательной программы (ОП)

Требования к результатам освоения образовательной программы (ОП) бакалавриата условиям ее реализации и срокам освоения определяется ФГОС по направлению подготовки

10.03.01 «Информационная безопасность», утвержденного Приказом Министерства образования и науки Российской Федерации от 01 декабря 2016 г. № 1515.

Выпускник, освоивший программу бакалавриата в соответствии с видами профессиональной деятельности, на которые ориентирована программа магистратуры, должен быть готов решать следующие профессиональные задачи:

эксплуатационная деятельность:

установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований;

администрирование подсистем информационной безопасности объекта;

участие в проведении аттестации объектов информатизации по требованиям безопасности информации и аудите информационной безопасности автоматизированных систем;

проектно-технологическая деятельность:

сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности;

проведение проектных расчетов элементов систем обеспечения информационной безопасности;

участие в разработке технологической и эксплуатационной документации;

проведение предварительного технико-экономического обоснования проектных расчетов;

экспериментально-исследовательская деятельность:

сбор, изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования;

проведение экспериментов по заданной методике, обработка и анализ их результатов;

проведение вычислительных экспериментов с использованием стандартных программных средств;

организационно-управленческая деятельность:

осуществление организационно-правового обеспечения информационной безопасности объекта защиты;

организация работы малых коллективов исполнителей;

участие в совершенствовании системы управления информационной безопасностью;

изучение и обобщение опыта работы других учреждений, организаций и предприятий в области защиты информации, в том числе информации ограниченного доступа;

контроль эффективности реализации политики информационной безопасности объекта защиты.

Результатами освоения ОП ВО являются сформированные у выпускника знания, умения, навыки (владения) в соответствии с видами деятельности ФГОС ВО по направлению подготовки 10.03.01 «Информационная безопасность» (таблица 1).

Таблица 1 – Результаты освоения ОП ВО

Компетенция		Результаты освоения ОП ВО
Код	Содержание	
1	2	3
Общекультурные		
ОК-1	способность использовать основы философских знаний для формирования мировоззренческой позиции	*Знать*: приемы философского анализа проблем. *Уметь*: анализировать проблемы и планировать свою деятельность с учетом результатов этого анализа. *Владеть*: навыками публичной речи, аргументации, ведения дискуссии и полемики, навыками письменного аргументированного изложения собственной точки зрения
ОК-2	способность использовать основы экономических знаний в различных сферах деятельности	*Знать*: основные понятия экономической деятельности в области защиты информации. *Уметь*: оценивать эффективность и анализировать экономические показатели в области защиты информации. *Владеть*: навыками экономического обоснования выбранного решения.
ОК-3	способность анализировать основные этапы и закономерности исторического развития России, ее место и роль в современном мире для формирования гражданской позиции и развития патриотизма	*Знать:* основные исторические аспекты развития системы защиты информации. *Уметь*: осуществлять эффективный поиск информации и критику источников. *Владеть*: приемами ведения дискуссии и полемики.
ОК-4	способность использовать основы правовых знаний в различных сферах деятельности	*Знать:* законодательство в области защиты информации. *Уметь*: использовать в практической деятельности правовые знания. *Владеть*: навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности.
ОК-5	способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению	*Знать:* основы российской правовой системы в области защиты информации, характеристики организации деятельности органов государственной власти в Российской Федерации, правовые основы обеспечения национальной безопасности

Компетенция		Результаты освоения ОП ВО
Код	Содержание	
1	2	3
	профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	Российской Федерации. *Уметь*: формулировать и аргументировано отстаивать собственную позицию по различным проблемам с соблюдением норм профессиональной этики. *Владеть*: приемами ведения дискуссии и полемики с соблюдением норм профессиональной этики.
ОК-6	способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия	*Знать*: основные понятия и методы в области управленческой деятельности. *Уметь*: осуществлять планирование и организацию работы коллектива при выполнении поставленных задач. *Владеть*: навыками обоснования, реализации и контроля результатов управленческих решений по организации работы коллектива.
ОК-7	способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности	*Знать*: иностранный язык в объеме, необходимом для получения профессиональной информации из зарубежных источников и общения на деловом уровне; профессиональную лексику иностранного языка в объеме, необходимом для общения, чтения и перевода иноязычных текстов в рамках делового общения в профессиональной деятельности; основные грамматические явления и структуры государственного (русского) языка, используемые в устном и письменном общении в профессиональной деятельности. *Уметь*: использовать иностранный язык в межличностном общении и профессиональной деятельности; соблюдать речевой этикет в ситуациях повседневного и делового общения (устанавливать и поддерживать контакты, завершить беседу, запрашивать и сообщать информацию). *Владеть*: основами публичной речи, перевода текстов по специальности; навыками грамотно и эффективно пользоваться источниками информации (справочной литературой, ресурсами Интернет); навыками выражения своего мнения в процессе делового общения на иностранном языке.
ОК-8	способность к самоорганизации и самообразованию	*Знать*: методы самоорганизации и самообразования, планирования своей деятельности. *Уметь*: осуществлять планирование и организацию собственной деятельности, осуществлять эффективный поиск информации. *Владеть*: навыками обоснования, реализации и контроля собственной деятельности, навыками систематизации и анализа информации.

Компетенция		Результаты освоения ОП ВО
Код	Содержание	
1	2	3
ОК-9	способность использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности	*Знать*: роль и значение физической культуры в системе научной организации труда, влияние условий и характера труда на выбор форм, методов и средств производственной физической культуры. Уметь: интегрировать полученные знания в формирование профессионально значимых умений и навыков. *Владеть*: средствами и методами укрепления индивидуального здоровья, физического самосовершенствования для успешной социально-культурной и профессиональной деятельности; методиками и методами самодиагностики, самооценки, средствами оздоровления для самокоррекции здоровья различными формами двигательной деятельности, удовлетворяющими потребности человека в рациональном использовании свободного времени.
Общепрофессиональные		
ОПК-1	способность анализировать физические явления и процессы для решения профессиональных задач	*Знать*: особенности физических эффектов и явлений, используемые для обеспечения информационной безопасности. *Уметь*: применять основные законы физики при решении практических задач. *Владеть*: навыками проведения физического эксперимента и обработки его результатов.
ОПК-2	способность применять соответствующий математический аппарат для решения профессиональных задач	*Знать*: основные методы решения задач профессиональной области и применением математических методов и моделей. *Уметь*: использовать математические методы и модели для решения прикладных задач. *Владеть*: навыками применения математического аппарата для решения прикладных задач в области защиты информации.
ОПК-3	способность применять положения электротехники, электроники и схемотехники для решения профессиональных задач	*Знать*: принципы работы современной радиоэлектронной аппаратуры и физические процессы, протекающие в них. *Уметь*: применять полученные знания при использовании механизмов и приборов. *Владеть*: навыками работы с основными измерительными приборами.
ОПК-4	способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	*Знать*: основные понятия информатики. *Уметь*: использовать программные и аппаратные средства современного компьютера. *Владеть*: навыками поиска информации в глобальной сети Интернет и работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов).
ОПК-5	способность использовать нормативные правовые	*Знать*: правовые основы обеспечения информационной безопасности.

Компетенция		Результаты освоения ОП ВО
Код	Содержание	
1	2	3
	акты в профессиональной деятельности	*Уметь*: применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности. *Владеть*: навыками работы с нормативными правовыми актами.
ОПК-6	способность применять приемы оказания первой помощи, методы и средства защиты персонала предприятия и населения в условиях чрезвычайных ситуаций, организовать мероприятия по охране труда и технике безопасности	*Знать*: опасные и вредные факторы системы «человек – среда обитания», методы анализа антропогенных опасностей. *Уметь*: анализировать и оценивать степень риска проявления факторов опасности системы «человек – среда обитания», осуществлять и контролировать выполнения требований по охране труда и безопасности жизнедеятельности. *Владеть*: навыками безопасного использования технических средств в профессиональной деятельности.
ОПК-7	способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	*Знать*: основные угрозы безопасности информации и модели нарушителя в информационных системах. *Уметь*: определять комплекс мер (правила, процедуры, практические приемы, руководящие методы, принципы, средства) для обеспечения информационной безопасности информационных систем. *Владеть*: навыками формальной постановки и решения задачи обеспечения информационной безопасности, навыками анализа информационной инфраструктуры информационной системы и ее безопасности.
Профессиональные компетенции, соответствующие видам профессиональной деятельности, на которые ориентирована программа бакалавриата: а) в эксплуатационной деятельности:		
ПК-1	способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	*Знать*: принципы организации информационных систем в соответствии с требованиями по защите информации. *Уметь*: анализировать и оценивать угрозы информационно безопасности объектов, использовать программные и аппаратные средства современного компьютера. *Владеть*: методами установки и настройки программно-аппаратных и технических средств защиты информации.
ПК-2	способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	*Знать*: принципы организации информационных систем в соответствии с требованиями по защите информации. *Уметь*: осуществлять меры противодействия нарушениям информационной безопасности. *Владеть*: профессиональной терминологией, навыками использования программных средств системного, прикладного и специального назначения.

Компетенция		Результаты освоения ОП ВО
Код	Содержание	
1	2	3
ПК-3	способность администрировать подсистемы информационной безопасности объекта защиты	*Знать*: принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации. *Уметь*: осуществлять меры противодействия нарушениям безопасности. *Владеть*: методикой анализа угроз безопасности информации.
ПК-4	способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	*Знать*: принципы организации информационных систем в соответствии с требования по защите информации. *Уметь*: определять информационную инфраструктуру и информационные ресурса организации, подлежащие защите. *Владеть*: навыками анализа информационной инфраструктуры информационной системы и ее безопасности.
ПК-5	способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	*Знать*: основные угрозы безопасности информации и модели нарушителя в информационных системах. *Уметь*: контролировать эффективность принятых мер по обеспечению информационной безопасности информационных систем. *Владеть*: навыками выбора и обоснования критериев эффективности функционирования защищенных информационных систем.
ПК-6	способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	*Знать*: основные методы управления информационной безопасностью, принципы формирования политики безопасности в информационных системах. *Уметь*: определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите, разрабатывать модели угроз и нарушителей информационной безопасности. *Владеть*: навыками выбора и обоснования критериев эффективности функционирования защищенных информационных систем.
б) в проектно-технологической деятельности		
ПК-7	способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих	*Знать*: современные угрозы безопасности информации и модели нарушителя в информационных системах. *Уметь*: разрабатывать модели угроз и нарушителей информационной безопасности информационных систем; выявлять уязвимости информационно-технологических ресурсов информационных систем, проводить мониторинг угроз безопасности информационных систем; оценивать информационные риски в информационных системах *Владеть*: методами мониторинга и аудита, выявле-

Компетенция		Результаты освоения ОП ВО
Код	Содержание	
1	2	3
	проектных решений	ния угроз информационной безопасности информационных систем; навыками выбора и обоснования критериев эффективности функционирования защищенных информационных систем.
ПК-8	способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	*Знать*: теоретические основы документоведения, структуру документов и нормативные требования к их оформлению. *Уметь*: составлять документы на любом носителе в зависимости от содержания, назначения и вида документа. *Владеть*: навыками работы с документами.
в) в области экспериментально-исследовательской деятельности		
ПК-9	способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	*Знать*: методы систематизации научно-технической информации, выбора методик и научных средств решения задач при решении прикладных проблем информационной безопасности. *Уметь*: разрабатывать планы и программы проведения научных исследований и технических разработок. *Владеть*: навыков сбора, обработки, анализа и систематизации научно-технической информации.
ПК-10	способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	*Знать*: основные отечественные и международные стандарты информационной безопасности. *Уметь*: самостоятельно анализировать отечественные и международные стандарты информационной безопасности. *Владеть*: навыками применения отечественных и международных стандартов информационной безопасности.
ПК-11	способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	*Знать*: основные понятия и методы математического анализа, теории вероятностей и математической статистики, основные понятия и методы математической логики и теории алгоритмов, дискретной математики; основные понятия, законы и модели электричества и магнетизма; основные понятия, законы и модели теории колебаний и волн, оптики, акустики; особенности физических эффектов и явлений, используемых для обеспечения информационной безопасности. *Уметь*: применять основные законы физики при решении практических задач; использовать математические методы и модели для решения прикладных задач; строить математические модели задач профессиональной области *Владеть*: навыками проведения физического эксперимента; методами количественного анализа процессов обработки, поиска и передачи информации

Компетенция		Результаты освоения ОП ВО
Код	Содержание	
1	2	3
ПК-12	способность принимать участие в проведении экспериментальных исследований системы защиты информации	*Знать*: методологию создания систем защиты информации. *Уметь*: определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите. *Владеть*: методами мониторинга и аудита, выявления угроз информационной безопасности.
г) в области организационно-управленческой деятельности		
ПК-13	способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	*Знать*: основные методы управления информационной безопасностью *Уметь*: определять комплекс мер (правила, процедуры, практические приемы, руководящие методы, принципы, средства) для обеспечения информационной безопасности информационных систем. *Владеть*: методами управления информационной безопасностью информационных систем.
ПК-14	способность организовывать работу малого коллектива исполнителей в профессиональной деятельности	*Знать*: основные понятия и методы в области управленческой деятельности; порядок выработки и реализации управленческих решений; состав системы управления и требования к ее элементам; содержание управленческой работы руководителя подразделения. *Уметь*: осуществлять планирование и организацию работы рабочего коллектива при выполнении поставленных задач; разрабатывать, реализовывать, оценивать и корректировать процессы управления информационной безопасностью. *Владеть*: навыками обоснования, выбора, реализации и контроля результатов управленческого решения
ПК-15	способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	*Знать*: основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации; правовые основы организации защиты информации конфиденциального характера; организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения технической защиты информации конфиденциального характера, по аттестации объектов информатизации и сертификации средств защиты информации. *Уметь*: применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирую-

Компетенция		Результаты освоения ОП ВО
Код	Содержание	
1	2	3
		щих работу по защите информации. *Владеть*: навыками работы с нормативными правовыми актами; методами организации и управления деятельностью служб защиты информации на предприятии; методами формирования требований по защите информации.
Профессионально-специализированные компетенции		
ПСК-1	способность формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности	*Знать*: основы российской правовой системы в области защиты информации, основные понятия и методы в области управленческой деятельности, основные понятия экономической деятельности в области защиты информации. *Уметь*: определять комплекс мер (правила, процедуры, практические приемы, руководящие методы, принципы, средства) для обеспечения информационной безопасности информационных систем. *Владеть*: методами управления информационной безопасностью информационных систем.
ПСК-2	способность принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия	*Знать*: принципы организации информационных систем в соответствии с требованиями по защите информации. *Уметь*: определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; разрабатывать модели угроз и нарушителей информационной безопасности информационных систем; выявлять уязвимости информационно-технологических ресурсов информационных систем, проводить мониторинг угроз безопасности информационных систем. *Владеть*: методами управления информационной безопасностью информационных систем.
ПСК-3	способность участвовать в разработке подсистемы управления информационной безопасностью	*Знать*: этапы проектирования систем, комплексов, средства и технологий управления информационной безопасностью. *Уметь*: формировать требования к проектированию систем, комплексов, средства и технологий управления информационной безопасностью. *Владеть*: навыками разработки систем, комплексов, средства и технологий управления информационной безопасностью с учетом особенностей объектов защиты
ПСК-4	способность собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности	*Знать*: современные угрозы безопасности информации и модели нарушителя в информационных системах. *Уметь*: разрабатывать модели угроз и нарушителей информационной безопасности информационных систем; выявлять уязвимости информационно-технологических ресурсов информационных систем, проводить мониторинг угроз безопасности инфор-

Компетенция		Результаты освоения ОП ВО
Код	Содержание	
1	2	3
		мационных систем; оценивать информационные риски в информационных системах *Владеть*: методами мониторинга и аудита, выявления угроз информационной безопасности информационных систем; навыками выбора и обоснования критериев эффективности функционирования защищенных информационных систем.
ПСК-5	способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью	*Знать*: принципы организации информационных систем в соответствии с требованиями по защите информации. *Уметь*: определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; разрабатывать модели угроз и нарушителей информационной безопасности информационных систем; выявлять уязвимости информационно-технологических ресурсов информационных систем, проводить мониторинг угроз безопасности информационных систем. *Владеть*: методами управления информационной безопасностью информационных систем.
ПСК-6	способность формировать комплекс мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью	*Знать*: принципы организации информационных систем в соответствии с требованиями по защите информации. *Уметь*: определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; разрабатывать модели угроз и нарушителей информационной безопасности информационных систем; выявлять уязвимости информационно-технологических ресурсов информационных систем, проводить мониторинг угроз безопасности информационных систем, определять комплекс мер (правила, процедуры, практические приемы, руководящие методы, принципы, средства) для обеспечения информационной безопасности информационных систем. *Владеть*: методами управления информационной безопасностью информационных систем.

4 Государственный экзамен

Государственный экзамен не предусмотрен.

5 Выпускная квалификационная работа

5.1 Требования к структуре, оформлению, порядку выполнения, критериям оценки, представлению к защите ВКР

Требования к структуре, оформлению, порядку выполнения, критериям оценки, представлению к защите выпускной квалификационной работы - единые по университету,

закреплены в стандарте университета СТО 2.3.5-2016 «Выпускная квалификационная работа: Требования к оформлению, порядок выполнения, критерии оценки».

5.2 Процедура защиты ВКР, регламент работы государственной экзаменационной комиссии

Процедура защиты ВКР, регламент работы государственной экзаменационной комиссии - единые по университету, закреплены в Положении ПЛ 2.3.23 – 2017 «Порядок проведения государственной итоговой аттестации по образовательным программам высшего образования – по программам бакалавриата, программам специалитета и программам магистратуры».

5.3 Примерный перечень тем ВКР

1) Разработка системы контроля доступа на промышленном предприятии.
2) Проектирование комплексной системы защиты информации на предприятии.
3) Адаптация информационных систем персональных данных к новым изменениям в законодательстве Российской Федерации.
4) Разработка и внедрение системы разграничения прав доступа в организации.
5) Разработка системы защиты информации при проведении видеоконференций.
6) Анализ эффективности применения пассивных и активных средств защиты информации при блокировании виброакустического канала утечки информации на предприятии.
7) Сравнительный анализ защищенности локальной вычислительной сети, основанной на операционных системах Windows и Linux.
8) Разработка комплекса мероприятий по организации защиты информации в коммерческой организации.
9) Анализ и минимизация информационного риска при передаче данных по сети общего пользования.
10) Методика построения модели нарушителя для предприятий различных форм собственности.
11) Адаптация изменений законодательства Российской Федерации по защите персональных данных к существующим информационным системам обработки персональных данных.
12) Анализ защищенности беспроводных локальных сетей на предприятии. Меры повышения защищенности.
13) Разработка системы защиты персональных данных в организации.

14) Проектирование системы резервного копирования для информационной системы высокой доступности.
15) Методы обнаружения вторжений и их применение в информационных системах, обрабатывающих информацию конфиденциального характера.
16) Разработка практического руководства по обеспечению информационной безопасности на предприятии.
17) Исследование методов повышения стойкости стеганографических систем.
18) Анализ эффективности применения технических средств для оценки характеристик защищенности помещений.
19) Разработка методики выявления скрытых каналов передачи информации посредством побочных электромагнитных излучений.
20) Разработка требований для подготовки предприятия к лицензированию его длительности по технической защите конфиденциальной информации.
21) Разработка мер противодействия угрозам безопасности корпоративной информации со стороны сотрудников предприятия.
22) Разработка методики противодействия современным атакам на информационные системы организации.
23) Разработка безопасного принципа проведения транзакций в системах электронной коммерции.
24) Применение облачных технологий в обеспечении информационной безопасности предприятия.
25) Методика оценки актуальности угроз информационной безопасности в государственных информационных системах.
26) Разработка документации по использованию систем обнаружения вторжений в комплексных системах защиты информации.
27) Проектирование защищенной системы дистанционного обучения.
28) Разработка и внедрение системы защиты периметра сети на предприятии.
29) Проектирование и анализ распределенной системы видеонаблюдения на предприятии.
30) Анализ информационной безопасности в автоматизированных системах управления на предприятии.
31) Модернизация системы контроля и управления доступом на типовом объекте транспортной инфраструктуры.
32) Анализ возможностей использования средств защиты информации в соответствии с требованиями руководящих документов.
33) Разработка и внедрение методов управления риском утечки информации из корпоративной сети предприятия.

34) Разработка методов противодействия лазерно-акустическим средствам разведки.
35) Подготовка и проведение аттестационных испытаний объекта информатизации по требованиям безопасности информации.
36) Анализ цифровых изображений с целью оптимизации стеганографического скрытия информации.
37) Внедрение системы защищенного электронного документооборота на предприятии.
38) Аудит информационной безопасности предприятия на соответствие международным стандартам.
39) Особенности применения операционных систем в качестве средства защиты от несанкционированного доступа к информации в ходе аттестации объектов вычислительной техники на соответствие требованиям по безопасности информации.
40) Разработка профиля защиты для Интернет-ресурса организации.
41) Разработка методов обеспечения безопасности мобильной связи при эксплуатации на предприятии.
42) Разработка политики безопасности персональных данных при их обработке в базах данных организации.
43) Разработка политики управления инцидентами информационной безопасности на предприятии.
44) Исследование встроенных механизмов защиты информации в операционных системах и соответствие их руководящим документам по безопасности.
45) Разработка организационных и технических мер защиты информации в автоматизированной системе управления производственными и технологическими процессами на критически важном объекте.

5.4 Показатели и критерии оценивания компетенций, шкала оценивания

При оценивании результатов выполнения и защиты ВКР используются критерии оценивания компетенций (таблица 2) и общие критерии оценки ВКР (таблица 3).

Результаты государственного аттестационного испытания определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Оценки «отлично», «хорошо», «удовлетворительно» означают успешное прохождение государственного аттестационного испытания.

Критерии выставления оценок по количеству набранных баллов на защите ВКР:

86-100 баллов – «Отлично» - представленные на защиту графический и письменный (текстовой) материалы выполнены в соответствии с нормативными документами и согласуются с требованиями, предъявляемыми к уровню подготовки специалиста. Защита

проведена выпускником грамотно с четким изложением содержания квалификационной работы и с достаточным обоснованием самостоятельности ее разработки. Ответы на вопросы членов экзаменационной комиссии даны в полном объеме. Отзыв руководителя – положительный, с оценкой не ниже «хорошо». Компетенции сформированы на эталонном уровне в соответствии с результатами оценивания компетенции, представленными в таблице 2.

76-85 баллов – «Хорошо» - представленные на защиту графический и письменный (текстовой) материалы выполнены в соответствии с нормативными документами, но имеют место незначительные отклонения от существующих требований. Защита проведена грамотно с достаточным обоснованием самостоятельности разработки, но с неточностями в изложении отдельных положений содержания квалификационной работы. Ответы на некоторые вопросы членов экзаменационной комиссии даны не в полном объеме. Отзыв руководителя – положительный, с оценкой не ниже «хорошо». Формирование компетенций достигает продвинутого уровня в соответствии с результатами оценивания компетенции, представленными в таблице 2.

61-75 баллов – «Удовлетворительно» - представленные на защиту графический и письменный (текстовой) материалы в целом выполнены в соответствии с нормативными документами, но имеют место отступления от существующих требований. Защита проведена выпускником с недочетами в изложении содержания квалификационной работы и в обосновании самостоятельности ее выполнения. На отдельные вопросы членов экзаменационной комиссии ответы не даны. В процессе защиты показана достаточная подготовка к профессиональной деятельности, но при защите квалификационной работы отмечены отдельные отступления от требований, предъявляемых к уровню подготовки выпускника университета. Отзыв руководителя – положительный, с оценкой не ниже «удовлетворительно». Освоен пороговый уровень формирования компетенций в соответствии с результатами оценивания компетенции, представленными в таблице 2.

0-60 баллов – «Неудовлетворительно» - представленные на защиту графический и письменный (текстовый) материалы в целом выполнены в соответствии с нормативными документами, имеют место нарушения существующих требований. Защита проведена выпускником на низком уровне и ограниченным изложением содержания работы и неубедительным обоснованием самостоятельности ее выполнения. На большую часть вопросов, заданных членами экзаменационной комиссии, ответов не последовало. Проявлена недостаточная профессиональная подготовка. В отзыве руководителя имеются существенные замечания. Сформированный уровень компетенций недостаточен для получения положительной оценки по результатам оценивания компетенции, представленных в таблице 2.

Таблица 2 – Критерии сформированности компетенций

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
ОК-1	способен использовать основы философских знаний для формирования мировоззренческой позиции	Четко сформулированы цель и задачи ВКР Представленная в ВКР информация систематизирована и структурирована. Присутствует логика в изложении содержания ВКР. Приведен подробный анализ альтернативных вариантов решения исследовательских задач. Быстро и уверенно отвечает на поставленные вопросы комиссии. Уверенно отстаивает свою точку зрения.	5 (отлично) /3 уровень (эталонный)
		Четко сформулированы цель и задачи ВКР. Представленная в ВКР информация систематизирована и структурирована Присутствует логика в изложении содержания ВКР. В целом успешный, но содержащий отдельные пробелы анализ альтернативных вариантов решения исследовательских задач. Быстро и уверенно отвечает на поставленные вопросы комиссии.	4 (хорошо) / 2 уровень (продвинутый)
		Нечетко сформулированы цель и задачи ВКР. Представленная в ВКР информация недостаточно систематизирована и не структурирована. Логика в изложении содержания ВКР присутствует фрагментарно.	3 (удовл.) /1 уровень (пороговый)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		В целом успешный, но не систематически осуществляемый анализ альтернативных вариантов решения исследовательских задач. Частично справляется с поставленными вопросами комиссии.	
		Не сформулированы цель и задачи ВКР. Представленная в ВКР информация не систематизирована и не структурирована. Отсутствует логика в изложении содержания ВКР. Отсутствует анализ альтернативных вариантов решения исследовательских задач. Не справляется с поставленными вопросами комиссии.	2 (неудовл.)
ОК-2	способен использовать основы экономических знаний в различных сферах деятельности	В экономическом разделе ВКР четко поставлена задача оценки экономической эффективности предложенных решений. Экономический анализ проведен полно и правильно. Полученные выводы обоснованы.	5 (отлично) /3 уровень (эталонный)
		В экономическом разделе ВКР четко поставлена задача оценки экономической эффективности предложенных решений. Экономический анализ содержит незначительные ошибки. Полученные выводы обоснованы.	4 (хорошо) / 2 уровень (продвинутый)
		В экономическом разделе ВКР четко поставлена задача оценки экономической эффективности предложенных решений.	3 (удовл.) /1 уровень (пороговый)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		Экономический анализ содержит незначительные ошибки. Полученные выводы частично обоснованы.	
		В экономическом разделе ВКР не поставлена задача оценки экономической эффективности предложенных решений. Экономический анализ содержит значительные ошибки. Полученные выводы необоснованы.	2 (неудовл.)
ОК-3	способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в современном мире для формирования гражданской позиции и развития патриотизма	В ВКР приведена краткая историческая справка по формированию и развитию рассматриваемой проблемы. Список использованных источников содержит более одной ссылки на литературу по истории проблемы.	5 (отлично) /3 уровень (эталонный)
		В ВКР приведена краткая историческая справка по формированию и развитию рассматриваемой проблемы. Список использованных источников содержит одну ссылку на литературу по истории проблемы.	4 (хорошо) / 2 уровень (продвинутый)
		В ВКР приведена краткая историческая справка по формированию и развитию рассматриваемой проблемы. Список использованных источников не содержит ссылок на литературу по истории проблемы.	3 (удовл.) /1 уровень (пороговый)
		В ВКР не приведена историческая справка по формированию и развитию рассматриваемой проблемы. Список использованных источников не содержит ссылок на литературу по истории проблемы.	2 (неудовл.)
ОК-4	способен	Опирается на нормативные	5 (отлично)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
	использовать основы правовых знаний в различных сферах деятельности	правовые акты в области информационной безопасности и защиты информации, нормативные методические документы ФСБ России, ФСТЭК России. В ВКР приведены проекты нормативно-распорядительных документов, регламентирующих работу по защите информации применительно к объекту исследования.	/3 уровень (эталонный)
		Опирается на нормативные правовые акты в области информационной безопасности и защиты информации, нормативные методические документы ФСБ России, ФСТЭК России.	4 (хорошо) / 2 уровень (продвинутый)
		При формулировке требований к обеспечению информационной безопасности объекта защиты приводит перечень соответствующих нормативных правовых актов в области информационной безопасности и защиты информации, нормативных методических документа ФСБ России, ФСТЭК России, но данный перечень неполон и не систематизирован.	3 (удовл.) /1 уровень (пороговый)
		Не ориентируется в нормативных правовых актах в области информационной безопасности и защиты информации, нормативных методических документах ФСБ России, ФСТЭК России.	2 (неудовл.)
ОК-5	способен понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к	При формулировке управленческого решения по организации внедрения результатов исследования в числе прочего опирается на нормативные правовые акты в	5 (отлично) /3 уровень (эталонный)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
	выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	области информационной безопасности и защиты информации, нормативные методические документы ФСБ России, ФСТЭК России. В ВКР приведены проекты нормативно-распорядительных документов, регламентирующих работу по защите информации применительно к объекту исследования. Быстро и уверенно отвечает на поставленные вопросы комиссии. Уверенно отстаивает свою точку зрения.	
		При формулировке управленческого решения по организации внедрения результатов исследования в числе прочего опирается на нормативные правовые акты в области информационной безопасности и защиты информации, нормативные методические документы ФСБ России, ФСТЭК России. Быстро и уверенно отвечает на поставленные вопросы комиссии.	4 (хорошо) / 2 уровень (продвинутый)
		При формулировке требований к обеспечению информационной безопасности объекта защиты приводит перечень соответствующих нормативных правовых актов в области информационной безопасности и защиты информации, нормативных методических документа ФСБ России, ФСТЭК России, но данный перечень неполон и не систематизирован. Частично справляется с поставленными вопросами	3 (удовл.) /1 уровень (пороговый)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		комиссии.	
		Не ориентируется в нормативных правовых актах в области информационной безопасности и защиты информации, нормативных методических документах ФСБ России, ФСТЭК России. Не справляется с поставленными вопросами комиссии.	2 (неудовл.)
ОК-6	способен работать в коллективе, толерантно воспринимая социальные, культурные и иные различия	При работе над ВКР проявил навыки четкого планирования своих действий и организации работ в коллективе, включающем руководителя ВКР и консультантов по разделам. Не допускал нарушения календарного плана. При общении с руководителем и консультантами соблюдал профессиональную этику.	5 (отлично) /3 уровень (эталонный)
		При работе над ВКР проявил навыки четкого планирования своих действий и организации работ в коллективе, включающем руководителя ВКР и консультантов по разделам. Допускал нарушения календарного плана. При общении с руководителем и консультантами соблюдал профессиональную этику.	4 (хорошо) / 2 уровень (продвинутый)
		При работе над ВКР не продемонстрировал навыки четкого планирования своих действий и организации работ в коллективе, включающем руководителя ВКР и консультантов по разделам. Допускал нарушения календарного плана. При общении с руководителем и консультантами соблюдал профессиональную этику.	3 (удовл.) /1 уровень (пороговый)
		При работе над ВКР не	2 (неудовл.)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		планировал свои действия и организацию работ в коллективе, включающем руководителя ВКР и консультантов по разделам. Допускал значительные нарушения календарного плана. При общении с руководителем и консультантами допускал нарушения профессиональной этики.	
ОК-7	способен к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности	Аннотация к ВКР а иностранном языке написана без ошибок. Грамотно и внятно строит доклад на государственном языке. Текст ВКР написан без ошибок. Все профессиональные термины на иностранном языке, встречающиеся в тексте ВКР правильно используются и трактуются. Ответы на вопросы комиссии грамотно и четко сформулированы, не вызывают затруднений.	5 (отлично) /3 уровень (эталонный)
		Аннотация к ВКР иностранном допущены ошибки. Грамотно и внятно строит доклад на государственном языке. Текст ВКР написан без ошибок. Все профессиональные термины на иностранном языке, встречающиеся в тексте ВКР правильно используются и трактуются. При ответе на вопросы комиссии возникают затруднения в формулировке своей мысли.	4 (хорошо) / 2 уровень (продвинутый)
		В аннотации к ВКР а иностранном языке допущены	3 (удовл.) /1 уровень

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		существенные ошибки. Достаточно грамотно строит свою речь на государственном языке. В тексте ВКР встречаются орфографические и синтаксические ошибки. Затрудняется в произношении и толковании профессиональных терминов на иностранном языке, встречающихся в тексте ВКР. При ответе на вопросы комиссии возникают затруднения в формулировке своей мысли.	(пороговый)
		Аннотация к ВКР на иностранном языке отсутствует. Не может внятно изложить свою мысль на государственном языке. В тексте ВКР допущены орфографические и синтаксические ошибки. Не может истолковать значения ни одного профессионального термина на иностранном языке, встречающегося в тексте ВКР. Не может сформулировать свою мысль при ответе на вопросы комиссии.	2 (неудовл.)
ОК-8	способен к самоорганизации и самообразованию	Список использованных источников достаточно объемен, систематизирован, отражает тематику всех разделов ВКР. Расстановка ссылок на использованные источники в тексте ВКР соответствует содержанию. Знания и умения, полученные из использованных источников, отражены в тексте ВКР и в докладе. Приведен полный анализ использованных источников.	5 (отлично) /3 уровень (эталонный)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		Список использованных источников достаточно объемен, систематизирован, отражает тематику всех разделов ВКР. Расстановка ссылок на использованные источники в тексте ВКР соответствует содержанию. Знания и умения, полученные из использованных источников, отражены в тексте ВКР и в докладе. Приведенный анализ использованных источников недостаточно полон (не отражены все использованные источники).	4 (хорошо) / 2 уровень (продвинутый)
		Список использованных источников систематизирован, но не отражает тематику всех разделов ВКР. Расстановка ссылок на использованные источники в тексте ВКР соответствует содержанию. Знания и умения, полученные из использованных источников, отражены в тексте ВКР и в докладе. Приведен частичный анализ использованных источников.	3 (удовл.) /1 уровень (пороговый)
		Список использованных источников составлен формально и несистематически. Ссылки на использованные источники в тексте ВКР расставлены случайным образом. Знания и умения, полученные из использованных источников, не отражены в тексте ВКР и в докладе. Отсутствует анализ использованных источников.	2 (неудовл.)
ОК-9	способен использовать методы	На защите ВКР выглядит бодрым и здоровым.	5 (отлично) /3 уровень

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
	и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности	Демонстрирует спокойствие и уверенность в себе. При работе над ВКР проявил высокую степень самоорганизованности. Не допускал нарушений календарного плана по причине нарушений здоровья из-за усталости.	(эталонный)
		На защите ВКР выглядит бодрым и здоровым. Демонстрирует спокойствие и уверенность в себе. При работе над ВКР проявил самоорганизованность. Не допускал нарушений календарного плана по причине нарушений здоровья из-за усталости.	4 (хорошо) / 2 уровень (продвинутый)
		На защите ВКР демонстрирует признаки неуверенности в себе и угнетенности. При работе над ВКР не проявил самоорганизованность. Допускал нарушения календарного плана по причине нарушений здоровья из-за усталости.	3 (удовл.) /1 уровень (пороговый)
		На защите ВКР демонстрирует признаки неуверенности в себе и угнетенности. При работе над ВКР не проявил самоорганизованность. Допускал значительные нарушения календарного плана по причине нарушений здоровья из-за усталости.	2 (неудовл.)
ОПК-1	способен анализировать физические явления и процессы для решения профессиональных задач	Демонстрирует глубокое понимание физических эффектов и явлений, используемых для обеспечения информационной безопасности с учетом особенностей объекта защиты. Приведен их подробный и обоснованный анализ.	5 (отлично) /3 уровень (эталонный)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		Демонстрирует понимание основных физических эффектов и явлений, используемых для обеспечения информационной безопасности.	4 (хорошо) / 2 уровень (продвинутый)
		Демонстрирует неполное понимание основных физических эффектов и явлений, используемых для обеспечения информационной безопасности.	3 (удовл.) /1 уровень (пороговый)
		Демонстрирует полное непонимание основных физических эффектов и явлений, используемых для обеспечения информационной безопасности.	2 (неудовл.)
ОПК-2	способен применять соответствующий математический аппарат для решения профессиональных задач	В ВКР обоснованно и правильно применяются математические методы исследования защищенности объектов.	5 (отлично) /3 уровень (эталонный)
		В ВКР обоснованно и в основном правильно, но с некоторыми ошибками применяются математические методы исследования защищенности объектов.	4 (хорошо) / 2 уровень (продвинутый)
		В ВКР применяются математические методы исследования защищенности объектов, но при этом допускаются существенные ошибки и неточности.	3 (удовл.) /1 уровень (пороговый)
		В ВКР не применяются или применяются с существенными ошибками математические методы исследования защищенности объектов.	2 (неудовл.)
ОПК-3	способен применять положения электротехники, электроники и схемотехники для решения профессиональных	Демонстрирует глубокие знания принципов работы современной радиоэлектронной аппаратуры и физических процессов, протекающих в них.	5 (отлично) /3 уровень (эталонный)
		Демонстрирует знания	4 (хорошо)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
	задач	принципов работы современной радиоэлектронной аппаратуры и физических процессов, протекающих в них.	/ 2 уровень (продвинутый)
		Демонстрирует поверхностные знания принципов работы современной радиоэлектронной аппаратуры и физических процессов, протекающих в них.	3 (удовл.) /1 уровень (пороговый)
		Не демонстрирует знаний принципов работы современной радиоэлектронной аппаратуры и физических процессов, протекающих в них.	2 (неудовл.)
ОПК-4	способен понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	При оформлении текста ВКР с использование текстового процессора использованы все необходимые функции по форматированию текста, таблиц, рисунков, формул. Презентационные материалы выполнены на профессиональном уровне.	5 (отлично) /3 уровень (эталонный)
		При оформлении текста ВКР с использование текстового процессора использованы все необходимые функции по форматированию текста, таблиц, рисунков, формул. Презентационные материалы выполнены на высоком уровне.	4 (хорошо) / 2 уровень (продвинутый)
		При оформлении текста ВКР с использование текстового процессора использованы базовые функции по форматированию текста, таблиц, рисунков, формул. Уровень презентационных материалов не способствует полноценному восприятию информации.	3 (удовл.) /1 уровень (пороговый)
		При оформлении текста ВКР с использование текстового	2 (неудовл.)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		процессора не использованы функции по форматированию текста, таблиц, рисунков, формул. Презентационные материалы отсутствуют.	
ОПК-5	способен использовать нормативные правовые акты в профессиональной деятельности	При формулировке управленческого решения по организации внедрения результатов исследования в числе прочего опирается на нормативные правовые акты в области информационной безопасности и защиты информации, нормативные методические документы ФСБ России, ФСТЭК России. В ВКР приведены проекты нормативно-распорядительных документов, регламентирующих работу по защите информации применительно к объекту исследования. Быстро и уверенно отвечает на поставленные вопросы комиссии. Уверенно отстаивает свою точку зрения.	5 (отлично) /3 уровень (эталонный)
		При формулировке управленческого решения по организации внедрения результатов исследования в числе прочего опирается на нормативные правовые акты в области информационной безопасности и защиты информации, нормативные методические документы ФСБ России, ФСТЭК России. Быстро и уверенно отвечает на поставленные вопросы комиссии.	4 (хорошо) / 2 уровень (продвинутый)
		При формулировке требований к обеспечению информационной безопасности объекта защиты	3 (удовл.) /1 уровень (пороговый)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		приводит перечень соответствующих нормативных правовых актов в области информационной безопасности и защиты информации, нормативных методических документа ФСБ России, ФСТЭК России, но данный перечень неполон и не систематизирован. Частично справляется с поставленными вопросами комиссии.	
		Не ориентируется в нормативных правовых актах в области информационной безопасности и защиты информации, нормативных методических документах ФСБ России, ФСТЭК России. Не справляется с поставленными вопросами комиссии.	2 (неудовл.)
ОПК-6	способен применять приемы оказания первой помощи, методы и средства защиты персонала предприятия и населения в условиях чрезвычайных ситуаций, организовать мероприятия по охране труда и технике безопасности	В разделе «Безопасность жизнедеятельности» четко поставлена. Раздел выполнен полно и правильно. Полученные выводы обоснованы.	5 (отлично) /3 уровень (эталонный)
		В разделе «Безопасность жизнедеятельности» четко поставлена. Раздел выполнен полно и правильно. Обоснование полученных выводов содержит несущественные ошибки.	4 (хорошо) / 2 уровень (продвинутый)
		В разделе «Безопасность жизнедеятельности» отсутствует четкая постановка задачи. Раздел выполнен не полно. Обоснование полученных выводов содержит существенные ошибки.	3 (удовл.) /1 уровень (пороговый)
		В разделе «Безопасность жизнедеятельности»	2 (неудовл.)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		отсутствует постановка задачи. Раздел выполнен не полно и с существенными ошибками. Обоснование полученных выводов отсутствует.	
ОПК-7	способен определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	В ВКР приведен анализ информационной инфраструктуры объекта защиты. Приведено подробное и структурированное описание модели угроз и модели нарушителя. Приведено описание политики безопасности объекта защиты, учитывающее его особенности. Определен комплекс мер (правил, процедур, практических приемов, руководящих принципов, методов, средств) для обеспечения информационной безопасности объекта защиты. В ВКР присутствует подробное описание управленческого решения по реализации полученных результатов, включая организационные мероприятия по его внедрению с описанием результатов внедрения. К ВКР прилагается акт внедрения предложенного решения на предприятии.	5 (отлично) /3 уровень (эталонный)
		В ВКР приведен анализ информационной инфраструктуры объекта защиты. Приведено подробное и структурированное описание модели угроз и модели нарушителя. Приведено описание политики безопасности объекта защиты, учитывающее его	4 (хорошо) / 2 уровень (продвинутый)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		особенности. Определен комплекс мер (правил, процедур, практических приемов, руководящих принципов, методов, средств) для обеспечения информационной безопасности объекта защиты. В ВКР присутствует подробное описание управленческого решения по реализации полученных результатов, включая организационные мероприятия по его внедрению с описанием результатов внедрения.	
		В ВКР приведен анализ информационной инфраструктуры объекта защиты. Приведено фрагментарное описание модели угроз и модели нарушителя. Приведено формальное описание политики безопасности объекта защиты. Меры (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности объекта защиты описаны полно, но не системно.	3 (удовл.) /1 уровень (пороговый)
		В ВКР не приводится анализ информационной инфраструктуры объекта защиты. Отсутствует описание модели угроз и модели нарушителя. Отсутствует описание политики безопасности объекта защиты. Меры (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для	2 (неудовл.)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		обеспечения информационной безопасности объекта защиты описаны фрагментарно.	
ПК-1	способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	При использовании в ВКР программных, программно-аппаратных и технических средств защиты информации их установка и настройка выполнялась полностью самостоятельно и без затруднений.	5 (отлично) /3 уровень (эталонный)
		При использовании в ВКР программных, программно-аппаратных и технических средств защиты информации их установка и настройка выполнялась с помощью руководителя и с незначительными затруднениями.	4 (хорошо) / 2 уровень (продвинутый)
		При использовании в ВКР программных, программно-аппаратных и технических средств защиты информации их установка и настройка выполнялась с помощью руководителя и с значительными затруднениями.	3 (удовл.) /1 уровень (пороговый)
		При использовании в ВКР программных, программно-аппаратных и технических средств защиты информации не смог самостоятельно выполнить их установку и настройку.	2 (неудовл.)
ПК-2	способен применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных	При использовании в ВКР программных средств системного, прикладного и специального назначения, инструментальные средства, языков и систем программирования применял их полностью самостоятельно.	5 (отлично) /3 уровень (эталонный)
		При использовании в ВКР программных средств системного, прикладного и специального назначения,	4 (хорошо) / 2 уровень (продвинутый)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
	задач	инструментальные средства, языков и систем программирования применял их с помощью руководителя и с незначительными затруднениями.	
		При использовании в ВКР программных средств системного, прикладного и специального назначения, инструментальные средства, языков и систем программирования применял их с помощью руководителя и с значительными затруднениями.	3 (удовл.) /1 уровень (пороговый)
		При использовании в ВКР программных средств системного, прикладного и специального назначения, инструментальные средства, языков и систем программирования не смог их применить самостоятельно.	2 (неудовл.)
ПК-3	способен администрировать подсистемы информационной безопасности объекта защиты	Демонстрирует четкое понимание процесса администрирования систем, комплексов, средств и технологий обеспечения информационной безопасности. В ВКР полно отражены требования к администрированию систем, комплексов, средств и технологий обеспечения информационной безопасности, являющихся объектов исследования. Продемонстрированы навыки администрирования систем, комплексов, средств и технологий обеспечения информационной безопасности с учетом особенностей объекта защиты.	5 (отлично) /3 уровень (эталонный)
		Допускает неточности в описании процесса	4 (хорошо) / 2 уровень

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		администрирования систем, комплексов, средств и технологий обеспечения информационной безопасности. В ВКР полно отражены требования к администрированию систем, комплексов, средств и технологий обеспечения информационной безопасности, являющихся объектов исследования. Продемонстрированы навыки администрирования систем, комплексов, средств и технологий обеспечения информационной безопасности.	(продвинутый)
		Имеет неполное представление об администрировании систем, комплексов, средств и технологий обеспечения информационной безопасности. В ВКР частично отражены требования к администрированию систем, комплексов, средств и технологий обеспечения информационной безопасности, являющихся объектов исследования. Продемонстрированы фрагментарные навыки администрирования систем, комплексов, средств и технологий обеспечения информационной безопасности.	3 (удовл.) /1 уровень (пороговый)
		Не имеет представления об администрировании систем, комплексов, средств и технологий обеспечения информационной безопасности. В ВКР не отражены	2 (неудовл.)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		требования к администрированию систем, комплексов, средств и технологий обеспечения информационной безопасности, являющихся объектов исследования. Не продемонстрированы навыки администрирования систем, комплексов, средств и технологий обеспечения информационной безопасности.	
ПК-4	способен участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	В ВКР приведен анализ информационной инфраструктуры объекта защиты. Приведено подробное и структурированное описание модели угроз и модели нарушителя. Приведено описание политики безопасности объекта защиты, учитывающее его особенности. Определен комплекс мер (правил, процедур, практических приемов, руководящих принципов, методов, средств) для обеспечения информационной безопасности объекта защиты. В ВКР присутствует подробное описание управленческого решения по реализации полученных результатов, включая организационные мероприятия по его внедрению с описанием результатов внедрения. К ВКР прилагается акт внедрения предложенного решения на предприятии.	5 (отлично) /3 уровень (эталонный)
		В ВКР приведен анализ информационной инфраструктуры объекта защиты.	4 (хорошо) / 2 уровень (продвинутый)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		Приведено подробное и структурированное описание модели угроз и модели нарушителя. Приведено описание политики безопасности объекта защиты, учитывающее его особенности. Определен комплекс мер (правил, процедур, практических приемов, руководящих принципов, методов, средств) для обеспечения информационной безопасности объекта защиты. В ВКР присутствует подробное описание управленческого решения по реализации полученных результатов, включая организационные мероприятия по его внедрению с описанием результатов внедрения.	
		В ВКР приведен анализ информационной инфраструктуры объекта защиты. Приведено фрагментарное описание модели угроз и модели нарушителя. Приведено формальное описание политики безопасности объекта защиты. Меры (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности объекта защиты описаны полно, но не системно.	3 (удовл.) /1 уровень (пороговый)
		В ВКР не приводится анализ информационной инфраструктуры объекта защиты. Отсутствует описание модели угроз и модели нарушителя.	2 (неудовл.)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		Отсутствует описание политики безопасности объекта защиты. Меры (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности объекта защиты описаны фрагментарно.	
ПК-5	способен принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	В ВКР приведен анализ информационной инфраструктуры объекта защиты. Приведено подробное и структурированное описание модели угроз и модели нарушителя. Приведено описание политики безопасности объекта защиты, учитывающее его особенности. Определен комплекс мер (правил, процедур, практических приемов, руководящих принципов, методов, средств) для обеспечения информационной безопасности объекта защиты. В ВКР присутствует подробное описание управленческого решения по реализации полученных результатов, включая организационные мероприятия по его внедрению с описанием результатов внедрения. К ВКР прилагается акт внедрения предложенного решения на предприятии.	5 (отлично) /3 уровень (эталонный)
		В ВКР приведен анализ информационной инфраструктуры объекта защиты. Приведено подробное и структурированное описание модели угроз и модели	4 (хорошо) / 2 уровень (продвинутый)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		нарушителя. Приведено описание политики безопасности объекта защиты, учитывающее его особенности. Определен комплекс мер (правил, процедур, практических приемов, руководящих принципов, методов, средств) для обеспечения информационной безопасности объекта защиты. В ВКР присутствует подробное описание управленческого решения по реализации полученных результатов, включая организационные мероприятия по его внедрению с описанием результатов внедрения.	
		В ВКР приведен анализ информационной инфраструктуры объекта защиты. Приведено фрагментарное описание модели угроз и модели нарушителя. Приведено формальное описание политики безопасности объекта защиты. Меры (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности объекта защиты описаны полно, но не системно.	3 (удовл.) /1 уровень (пороговый)
		В ВКР не приводится анализ информационной инфраструктуры объекта защиты. Отсутствует описание модели угроз и модели нарушителя. Отсутствует описание политики безопасности объекта защиты.	2 (неудовл.)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		Меры (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности объекта защиты описаны фрагментарно.	
ПК-6	способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	В ВКР приведен анализ информационной инфраструктуры объекта защиты. Приведено подробное и структурированное описание модели угроз и модели нарушителя. Приведено описание политики безопасности объекта защиты, учитывающее его особенности. Определен комплекс мер (правил, процедур, практических приемов, руководящих принципов, методов, средств) для обеспечения информационной безопасности объекта защиты. В ВКР присутствует подробное описание управленческого решения по реализации полученных результатов, включая организационные мероприятия по его внедрению с описанием результатов внедрения. К ВКР прилагается акт внедрения предложенного решения на предприятии.	5 (отлично) /3 уровень (эталонный)
		В ВКР приведен анализ информационной инфраструктуры объекта защиты. Приведено подробное и структурированное описание модели угроз и модели нарушителя. Приведено описание политики безопасности объекта защиты,	4 (хорошо) / 2 уровень (продвинутый)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		учитывающее его особенности. Определен комплекс мер (правил, процедур, практических приемов, руководящих принципов, методов, средств) для обеспечения информационной безопасности объекта защиты. В ВКР присутствует подробное описание управленческого решения по реализации полученных результатов, включая организационные мероприятия по его внедрению с описанием результатов внедрения.	
		В ВКР приведен анализ информационной инфраструктуры объекта защиты. Приведено фрагментарное описание модели угроз и модели нарушителя. Приведено формальное описание политики безопасности объекта защиты. Меры (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности объекта защиты описаны полно, но не системно.	3 (удовл.) /1 уровень (пороговый)
		В ВКР не приводится анализ информационной инфраструктуры объекта защиты. Отсутствует описание модели угроз и модели нарушителя. Отсутствует описание политики безопасности объекта защиты. Меры (правила, процедуры, практические приемы, руководящие принципы,	2 (неудовл.)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		методы, средства) для обеспечения информационной безопасности объекта защиты описаны фрагментарно.	
ПК-7	способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	Приведен полный анализ уязвимостей объекта защиты на обобщенном уровне. Построены детальные модели угроз и нарушителя используются, применительно к конкретному объекту защиты, с учетом современных проблем информационной безопасности. Приводятся ссылки на современные фундаментальные научные исследования в области разработки методик анализа угроз информационной безопасности и оценки уязвимостей.	5 (отлично) /3 уровень (эталонный)
		Приведен полный анализ уязвимостей объекта защиты на обобщенном уровне. Построены детальные модели угроз и нарушителя используются, применительно к конкретному объекту защиты, с учетом современных проблем информационной безопасности.	4 (хорошо) / 2 уровень (продвинутый)
		Приведен анализ уязвимостей объекта защиты на обобщенном уровне. В качестве модели угроз и модели нарушителя используются типовые модели, не учитываются современные проблемы информационной безопасности.	3 (удовл.) /1 уровень (пороговый)
		Допускает ошибки в классификации угроз информационной безопасности, их источников и	2 (неудовл.)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		последствий. В ВКР отсутствует построение модели нарушителя и анализ уязвимостей объекта защиты.	
ПК-8	способен оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	В списке использованных источников и в тексте ВКР имеются ссылки на источники научно-технической информации, проведен их критический анализ. Оформление текста пояснительной записки ВКР соответствует установленным требованиям. В списке использованных источников присутствует более одной ссылки на собственные публикации в научных изданиях и (или) апробацию результатов своей научно-исследовательской деятельности на научно-практических конференциях.	5 (отлично) /3 уровень (эталонный)
		В списке и в тексте ВКР использованных источников имеются ссылки на источники научно-технической информации. Оформление текста пояснительной записки ВКР соответствует установленным требованиям. В списке использованных источников присутствует хотя бы одна ссылка на собственную публикацию в научном издании и (или) апробацию результатов своей научно-исследовательской деятельности на научно-практической конференции.	4 (хорошо) / 2 уровень (продвинутый)
		В списке и в тексте ВКР использованных источников имеются ссылки на источники научно-технической информации. Оформление текста пояснительной записки ВКР	3 (удовл.) /1 уровень (пороговый)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		не полностью соответствует установленным требованиям. В списке использованных источников отсутствуют ссылки на собственные публикации в научных изданиях и (или) апробацию результатов своей научно-исследовательской деятельности на научно-практических конференциях.	
		В списке и в тексте ВКР использованных источников отсутствуют ссылки на источники научно-технической информации. Оформление текста пояснительной записки ВКР не соответствует установленным требованиям. В списке использованных источников отсутствуют ссылки на собственные публикации в научных изданиях и (или) апробацию результатов своей научно-исследовательской деятельности на научно-практических конференциях.	2 (неудовл.)
ПК-9	способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	Приводятся ссылки на современные фундаментальные научные исследования в области разработки методик анализа угроз информационной безопасности и оценки уязвимостей. Проведен их подробный обзор и анализ.	5 (отлично) /3 уровень (эталонный)
		Приводятся ссылки на современные фундаментальные научные исследования в области разработки методик анализа угроз информационной безопасности и оценки уязвимостей. Проведен их частичный обзор	4 (хорошо) / 2 уровень (продвинутый)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		и анализ.	
		Приводятся ссылки на современные фундаментальные научные исследования в области разработки методик анализа угроз информационной безопасности и оценки уязвимостей. Проведен их фрагментарный обзор и анализ.	3 (удовл.) /1 уровень (пороговый)
		Не приводятся ссылки на современные фундаментальные научные исследования в области разработки методик анализа угроз информационной безопасности и оценки уязвимостей.	2 (неудовл.)
ПК-10	способен проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	В тексте ВКР и в докладе приведен подробный анализ российских и (или) международных стандартов в области информационной безопасности. Применение стандартов к объекту исследования полностью обоснованно. Подробно отвечает на вопросы комиссии о содержании стандартов.	5 (отлично) /3 уровень (эталонный)
		В тексте ВКР и в докладе приведен подробный анализ российских и (или) международных стандартов в области информационной безопасности. Применение стандартов к объекту исследования обоснованно. При ответе на вопросы комиссии о содержании стандартов возникают затруднения.	4 (хорошо) / 2 уровень (продвинутый)
		В тексте ВКР и в докладе присутствуют ссылки на российские и (или) международные стандарты в	3 (удовл.) /1 уровень (пороговый)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		области информационной безопасности. Анализ стандартов не приводится.	
		В тексте ВКР и в докладе отсутствуют ссылки на российские и международные стандарты в области информационной безопасности. Стандарты в области информационной безопасности не анализируются и не применяются.	2 (неудовл.)
ПК-11	способен проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	Результаты экспериментов, проведенных в ходе работы над ВКР обработаны с применением профессиональных технических и (или) программных средств.	5 (отлично) /3 уровень (эталонный)
		Результаты экспериментов, проведенных в ходе работы над ВКР обработаны с применением базовых технических и (или) программных средств.	4 (хорошо) / 2 уровень (продвинутый)
		Результаты экспериментов, проведенных в ходе работы над ВКР обработаны без применения технических и (или) программных средств.	3 (удовл.) /1 уровень (пороговый)
		Результаты экспериментов, проведенных в ходе работы над ВКР не обработаны.	2 (неудовл.)
ПК-12	способен принимать участие в проведении экспериментальных исследований системы защиты информации	В ВКР приведены результаты экспериментальных исследований. Их описание четкое и обоснованное.	5 (отлично) /3 уровень (эталонный)
		В ВКР приведены результаты экспериментальных исследований. В их описании допущены незначительные ошибки.	4 (хорошо) / 2 уровень (продвинутый)
		В ВКР приведены результаты экспериментальных	3 (удовл.) /1 уровень

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		исследований. В их описании допущены значительные ошибки.	(пороговый)
		В ВКР не приведены результаты экспериментальных исследований.	2 (неудовл.)
ПК-13	способен принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	В ВКР присутствует подробное описание управленческого решения по реализации полученных результатов, включая организационные мероприятия по его внедрению с описанием результатов внедрения. К ВКР прилагается акт внедрения предложенного решения на предприятии.	5 (отлично) /3 уровень (эталонный)
		В ВКР присутствует подробное описание управленческого решения по реализации полученных результатов, включая организационные мероприятия по его внедрению с описанием результатов внедрения.	4 (хорошо) / 2 уровень (продвинутый)
		В ВКР присутствует теоретическое обоснование управленческого решения по реализации полученных результатов, включая организационные мероприятия по его внедрению.	3 (удовл.) /1 уровень (пороговый)
		В ВКР не приведено управленческое решение по реализации полученных результатов.	2 (неудовл.)
ПК-14	способен организовывать работу малого коллектива исполнителей в профессиональной деятельности	При работе над ВКР проявил навыки четкого планирования своих действий и организации работ в коллективе, включающем руководителя ВКР и консультантов по разделам. Не допускал нарушения	5 (отлично) /3 уровень (эталонный)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		календарного плана. При общении с руководителем и консультантами соблюдал профессиональную этику.	
		При работе над ВКР проявил навыки четкого планирования своих действий и организации работ в коллективе, включающем руководителя ВКР и консультантов по разделам. Допускал нарушения календарного плана. При общении с руководителем и консультантами соблюдал профессиональную этику.	4 (хорошо) / 2 уровень (продвинутый)
		При работе над ВКР не продемонстрировал навыки четкого планирования своих действий и организации работ в коллективе, включающем руководителя ВКР и консультантов по разделам. Допускал нарушения календарного плана. При общении с руководителем и консультантами соблюдал профессиональную этику.	3 (удовл.) /1 уровень (пороговый)
		При работе над ВКР не планировал свои действия и организацию работ в коллективе, включающем руководителя ВКР и консультантов по разделам. Допускал значительные нарушения календарного плана. При общении с руководителем и консультантами допускал нарушения профессиональной этики.	2 (неудовл.)
ПК-15	способен организовывать технологический процесс защиты информации ограниченного доступа в	При формулировке управленческого решения по организации внедрения результатов исследования в числе прочего опирается на нормативные правовые акты в области информационной	5 (отлично) /3 уровень (эталонный)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
	соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	безопасности и защиты информации, нормативные методические документы ФСБ России, ФСТЭК России. В ВКР приведены проекты нормативно-распорядительных документов, регламентирующих работу по защите информации применительно к объекту исследования.	
		При формулировке управленческого решения по организации внедрения результатов исследования в числе прочего опирается на нормативные правовые акты в области информационной безопасности и защиты информации, нормативные методические документы ФСБ России, ФСТЭК России.	4 (хорошо) / 2 уровень (продвинутый)
		При формулировке требований к обеспечению информационной безопасности объекта защиты приводит перечень соответствующих нормативных правовых актов в области информационной безопасности и защиты информации, нормативных методических документа ФСБ России, ФСТЭК России, но данный перечень неполон и не систематизирован.	3 (удовл.) /1 уровень (пороговый)
		Не ориентируется в нормативных правовых актах в области информационной безопасности и защиты информации, нормативных методических документах ФСБ России, ФСТЭК России.	2 (неудовл.)
ПСК-1	способен формировать комплекс мер по информационной	В ВКР приведен анализ информационной инфраструктуры объекта защиты.	5 (отлично) /3 уровень (эталонный)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
	безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности	Приведено подробное и структурированное описание модели угроз и модели нарушителя. Приведено описание политики безопасности объекта защиты, учитывающее его особенности. Определен комплекс мер (правил, процедур, практических приемов, руководящих принципов, методов, средств) для обеспечения информационной безопасности объекта защиты. В ВКР присутствует подробное описание управленческого решения по реализации полученных результатов, включая организационные мероприятия по его внедрению с описанием результатов внедрения. К ВКР прилагается акт внедрения предложенного решения на предприятии.	
		В ВКР приведен анализ информационной инфраструктуры объекта защиты. Приведено подробное и структурированное описание модели угроз и модели нарушителя. Приведено описание политики безопасности объекта защиты, учитывающее его особенности. Определен комплекс мер (правил, процедур, практических приемов, руководящих принципов, методов, средств) для обеспечения информационной безопасности объекта защиты. В ВКР присутствует подробное описание	4 (хорошо) / 2 уровень (продвинутый)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		управленческого решения по реализации полученных результатов, включая организационные мероприятия по его внедрению с описанием результатов внедрения.	
		В ВКР приведен анализ информационной инфраструктуры объекта защиты. Приведено фрагментарное описание модели угроз и модели нарушителя. Приведено формальное описание политики безопасности объекта защиты. Меры (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности объекта защиты описаны полно, но не системно.	3 (удовл.) /1 уровень (пороговый)
		В ВКР не приводится анализ информационной инфраструктуры объекта защиты. Отсутствует описание модели угроз и модели нарушителя. Отсутствует описание политики безопасности объекта защиты. Меры (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности объекта защиты описаны фрагментарно.	2 (неудовл.)
ПСК-2	способен принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия	Четко формулирует принципы обеспечения информационной безопасности, может привести примеры методик тестирования средств обеспечения информационной безопасности.	5 (отлично) /3 уровень (эталонный)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		Не допускает ошибок в классификации угроз информационной безопасности, их источников и последствий. При использовании средств обеспечения информационной безопасности в полном объеме учитывает установленные требования. В ВКР присутствуют подробная и обоснованная программа и (или) методика испытаний предложенных средств и систем обеспечения информационной безопасности.	
		Четко формулирует принципы обеспечения информационной безопасности, может привести примеры методик тестирования средств обеспечения информационной безопасности. Не допускает ошибок в классификации угроз информационной безопасности, их источников и последствий. При использовании средств обеспечения информационной безопасности в полном объеме учитывает установленные требования. В ВКР присутствуют элементы программы и (или) методики испытаний предложенных средств и систем обеспечения информационной безопасности.	4 (хорошо) / 2 уровень (продвинутый)
		Четко формулирует принципы обеспечения информационной безопасности, может привести примеры методик тестирования средств обеспечения информационной безопасности.	3 (удовл.) /1 уровень (пороговый)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		Не допускает ошибок в классификации угроз информационной безопасности, их источников и последствий. При использовании средств обеспечения информационной безопасности не в полном объеме учитывает установленные требования. В ВКР отсутствует программа и (или) методика испытаний предложенных средств и систем обеспечения информационной безопасности.	
		Не может сформулировать принципы обеспечения информационной безопасности, привести примеры методик тестирования средств обеспечения информационной безопасности. Допускает ошибки в классификации угроз информационной безопасности, их источников и последствий. При использовании средств обеспечения информационной безопасности не учитывает установленные требования. В ВКР отсутствует программа и (или) методика испытаний предложенных средств и систем обеспечения информационной безопасности.	2 (неудовл.)
ПСК-3	способен участвовать в разработке подсистемы управления информационной безопасностью	В ВКР разработана одна из подсистем управления информационной безопасностью.	5 (отлично) /3 уровень (эталонный)
		В ВКР приведены элементы разработки одной из подсистем управления информационной безопасностью.	4 (хорошо) / 2 уровень (продвинутый)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		В ВКР не приведена разработка подсистемы управления информационной безопасности.	3 (удовл.) /1 уровень (пороговый)
		Не имеет представления о подсистемах управления информационной безопасностью	2 (неудовл.)
ПСК-4	способен собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности	Приведен полный анализ уязвимостей объекта защиты на обобщенном уровне. Построены детальные модели угроз и нарушителя используются, применительно к конкретному объекту защиты, с учетом современных проблем информационной безопасности. Приводятся ссылки на современные фундаментальные научные исследования в области разработки методик анализа угроз информационной безопасности и оценки уязвимостей.	5 (отлично) /3 уровень (эталонный)
		Приведен полный анализ уязвимостей объекта защиты на обобщенном уровне. Построены детальные модели угроз и нарушителя используются, применительно к конкретному объекту защиты, с учетом современных проблем информационной безопасности.	4 (хорошо) / 2 уровень (продвинутый)
		Приведен анализ уязвимостей объекта защиты на обобщенном уровне. В качестве модели угроз и модели нарушителя используются типовые модели, не учитываются современные проблемы информационной безопасности.	3 (удовл.) /1 уровень (пороговый)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		Допускает ошибки в классификации угроз информационной безопасности, их источников и последствий. В ВКР отсутствует построение модели нарушителя и анализ уязвимостей объекта защиты.	2 (неудовл.)
ПСК-5	способен разрабатывать предложения по совершенствованию системы управления информационной безопасностью	В ВКР присутствует подробное описание управленческого решения по реализации полученных результатов, включая организационные мероприятия по его внедрению с описанием результатов внедрения. К ВКР прилагается акт внедрения предложенного решения на предприятии.	5 (отлично) /3 уровень (эталонный)
		В ВКР присутствует подробное описание управленческого решения по реализации полученных результатов, включая организационные мероприятия по его внедрению с описанием результатов внедрения.	4 (хорошо) / 2 уровень (продвинутый)
		В ВКР присутствует теоретическое обоснование управленческого решения по реализации полученных результатов, включая организационные мероприятия по его внедрению.	3 (удовл.) /1 уровень (пороговый)
		В ВКР не приведено управленческое решение по реализации полученных результатов.	2 (неудовл.)
ПСК-6	способен формировать комплекс мер (правила, процедуры, практические приемы и пр.) для управления информационной	В ВКР разработана одна из подсистем управления информационной безопасностью.	5 (отлично) /3 уровень (эталонный)
		В ВКР приведены элементы разработки одной из подсистем управления	4 (хорошо) / 2 уровень (продвинутый)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
	безопасностью	информационной безопасностью.	
		В ВКР не приведена разработка подсистемы управления информационной безопасности.	3 (удовл.) /1 уровень (пороговый)
		Не имеет представления о подсистемах управления информационной безопасностью	2 (неудовл.)

Члены комиссии оценивают выступление и ответы на вопросы защищающего по стобальной шкале (каждый показатель максимум 10 баллов) по показателям:

– Актуальность и обоснование выбора темы.

– Степень завершенности работы.

– Обоснованность полученных результатов и выводов.

– Теоретическая и практическая значимость работы.

– Применение новых технологий.

– Качество доклада (композиция, полнота представления работы, убежденность автора).

– Качество оформления ВКР и демонстрационных материалов.

– Культура речи, манера общения.

– Умение использовать наглядные пособия, способность заинтересовать аудиторию.

– Ответы на вопросы: полнота, аргументированность, убежденность, умение использовать ответы на вопросы для более полного раскрытия содержания проведенной работы.

Критерии оценивания компетенций, демонстрируемых при защите ВКР (таблица 3), а также шкалы оценивания сформированности компетенций описаны далее по тексту.

Таблица 3 – Общие критерии оценивания ВКР

Наименование общего показателя (критерия)	Критерии оценивания	Оценка (в баллах)/ уровень
Актуальность и обоснование выбора темы	Тема актуальна, выбор темы обоснован, результаты могут быть внедрены на	5 (отлично) /3 уровень

Наименование общего показателя (критерия)	Критерии оценивания	Оценка (в баллах)/ уровень
	производстве	(эталонный)
	Тема актуальна, выбор темы обоснован, после незначительной доработки результаты могут быть внедрены на производстве	4 (хорошо) / 2 уровень (продвинутый)
	Тема актуальна, допущены неточности при раскрытии причин выбора и актуальности темы	3 (удовл.) /1 уровень (пороговый)
	Тема не актуальна	2 (неудовл.)
Степень завершенности работы	Работа завершена полностью	5 (отлично) /3 уровень (эталонный)
	Работа завершена, но есть замечания	4 (хорошо) / 2 уровень (продвинутый)
	Работа завершена, но есть серьезные ошибки	3 (удовл.) /1 уровень (пороговый)
	Работа не завершена	2 (неудовл.)
Обоснованность полученных результатов и выводов	Анализ результатов верный, результаты достоверны, рекомендации соответствуют выводам	5 (отлично) /3 уровень (эталонный)
	Анализ результатов верный, результаты достоверны, рекомендации содержат ошибочные выводы	4 (хорошо) / 2 уровень (продвинутый)
	Анализ результатов содержит ошибочные суждения, рекомендации также содержат ошибочные суждения	3 (удовл.) /1 уровень (пороговый)
	Отсутствует обоснованность полученных результатов и выводов	2 (неудовл.)
Теоретическая и практическая значимость	К ВКР прилагается акт внедрения предложенного решения на предприятии	5 (отлично) /3 уровень (эталонный)
	В ВКР присутствуют подробные рекомендации по внедрению полученных результатов на предприятии	4 (хорошо) / 2 уровень (продвинутый)
	В ВКР присутствуют элементы рекомендаций по внедрению полученных результатов на предприятии	3 (удовл.) /1 уровень (пороговый)
	В ВКР не приведены рекомендации по внедрению полученных результатов на предприятии	2 (неудовл.)
Применение новых технологий	Применены и обоснованы с научной точки зрения новые технологии	5 (отлично) /3 уровень (эталонный)

Наименование общего показателя (критерия)	Критерии оценивания	Оценка (в баллах)/ уровень
	Применены новые технологии	4 (хорошо) / 2 уровень (продвинутый)
	Применены технологии, которые потеряли свою актуальность	3 (удовл.) /1 уровень (пороговый)
	Нет применения новых технологий	2 (неудовл.)
Качество доклада (композиция, полнота представления работы, убежденность автора)	Доклад структурирован, работа представлена полностью, доклад со стороны автора убедителен	5 (отлично) /3 уровень (эталонный)
	Доклад структурирован, работа представлена полностью, доклад со стороны автора недостаточно убедителен	4 (хорошо) / 2 уровень (продвинутый)
	Работа представлена полностью, доклад структурирован, доклад со стороны автора неубедителен, длительность выступления превышает регламент	3 (удовл.) /1 уровень (пороговый)
	Работа представлена не полностью, выступление не структурировано, недостаточно раскрываются причины выбора и актуальность темы	2 (неудовл.)
Качество оформления ВКР и демонстрационных материалов	Оформление ВКР и демонстрационных материалов в полной мере соответствует требованиям	5 (отлично) /3 уровень (эталонный)
	Оформление ВКР и демонстрационных материалов соответствует требованиям с небольшими замечаниями	4 (хорошо) / 2 уровень (продвинутый)
	Оформление ВКР и демонстрационных материалов не в полной мере соответствует требованиям	3 (удовл.) /1 уровень (пороговый)
	Оформление ВКР и демонстрационных материалов не соответствует требованиям	2 (неудовл.)
Культура речи, манера общения	В ходе доклада доходчиво доносит до членов комиссии суть рассматриваемых в ВКР проблем. При общении с членами комиссии полностью контролирует свое эмоциональное состояние, не нарушает морально-этические нормы делового общения	5 (отлично) /3 уровень (эталонный)
	В ходе доклада доходчиво доносит до членов комиссии суть рассматриваемых в ВКР проблем. При общении с членами комиссии полностью контролирует свое эмоциональное состояние, не нарушает морально-этические нормы делового	4 (хорошо) / 2 уровень (продвинутый)

Наименование общего показателя (критерия)	Критерии оценивания	Оценка (в баллах)/ уровень
	общения	
	В ходе доклада не может доходчиво донести до членов комиссии суть рассматриваемых в ВКР проблем. При общении с членами комиссии испытывает трудности в регулировании своего эмоционального состояния	3 (удовл.) /1 уровень (пороговый)
	В ходе доклада не может доходчиво донести до членов комиссии суть рассматриваемых в ВКР проблем. При общении с членами комиссии демонстрирует неспособность регулировать свое эмоциональное состояние, допускает нарушение морально-этических норм делового общения	2 (неудовл.)
Умение использовать наглядные пособия, способность заинтересовать аудиторию	Умеет использовать наглядные пособия, способен заинтересовать аудиторию	5 (отлично) /3 уровень (эталонный)
	Недостаточно эффективно умеет использовать наглядные пособия, способен заинтересовать аудиторию	4 (хорошо) / 2 уровень (продвинутый)
	Недостаточно эффективно умеет использовать наглядные пособия, не способен заинтересовать аудиторию	3 (удовл.) /1 уровень (пороговый)
	Отсутствует умение использовать презентации при защите ВКР, не способен заинтересовать аудиторию	2 (неудовл.)
Ответы на вопросы: полнота, аргументированность, убежденность, умение использовать ответы на вопросы для более полного раскрытия содержания проведенной работы	Ответы полные, аргументированные, умеет убеждать, присутствует умение использовать ответы на вопросы для более полного раскрытия содержания проведенной работы	5 (отлично) /3 уровень (эталонный)
	Ответы полные, аргументированные, но не умеет убеждать, отсутствует умение использовать ответы на вопросы для более полного раскрытия содержания проведенной работы	4 (хорошо) / 2 уровень (продвинутый)
	Минимальный ответ, ответы не раскрывают до конца сущности вопроса, слабо подкрепляются положениями нормативных правовых актов, выводами и расчетами из ВКР	3 (удовл.) /1 уровень (пороговый)
	Ответы не раскрывают сущности вопроса, не подкрепляются положениями нормативных правовых актов, выводами и расчетами из ВКР	2 (неудовл.)

Шкала оценивания сформированности компетенций.

Если хотя бы одно из лиц, оценивающих сформированность компетенций, считает, что хотя бы одна из компетенций, закрепленных за ГИА, сформирована ниже порогового уровня, работа в целом оценивается на «неудовлетворительно».

Если среднее арифметическое уровней освоения компетенций, закрепленных за ГИА, соответствует пороговому уровню, работа в целом оценивается на «удовлетворительно».

Если среднее арифметическое уровней освоения компетенций, закрепленных за ГИА, соответствует продвинутому уровню, работа в целом оценивается на «хорошо».

Если среднее арифметическое уровней освоения компетенций, закрепленных за ГИА, соответствует эталонному уровню, работа в целом оценивается на «отлично».

5.5 Перечень источников литературы при выполнении выпускной квалификационной работы

Перечень источников литературы, которую рекомендуется использовать при выполнении выпускной квалификационной работы по выбранной теме, приведен в таблице 4.

Таблица 4 – Перечень источников литературы

Основная литература						
№ п/п	Авторы, составители	Заглавие	Издательство, год	Кол-во. экз.	Кол-во. точек	Web-ссылка
1	Глухов М. М., Круглов И. А., Пикчур А. Б., Черемушкин А. В.	Введение в теоретико-числовые методы криптографии: учебное пособие : допущено УМО вузов по образованию в области информационной безопасности в качестве учебного пособия для студентов высших учебных заведений, обучающихся по специальности «Криптография»	Санкт-Петербург: Лань, 2011	-	29	http://e.lanbook.com/books/element.php?pl1_id=68466
2	Бородин А. Н.	Случайные процессы	Москва: Лань, 2013	-	29	http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=12935

3		Электричество и магнетизм. Волны. Оптика	Москва: Лань", 2016	-	29	http://e.lanbook.com/books/element.php?pl1_id=71761
4		Квантовая оптика. Атомная физика. Физика твердого тела. Физика атомного ядра и элементарных частиц	Москва: Лань", 2016	-	29	http://e.lanbook.com/books/element.php?pl1_id=71763
5	Акулич И. Л.	Математическое программирование в примерах и задачах: учеб. пособие	Москва: Лань, 2011	-	29	http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=2027
6	Невежин В. П.	Теория игр. Примеры и задачи: Учебное пособие	Москва: Издательство "ФОРУМ", 2014	-	29	http://znanium.com/go.php?id=426982
7	Геут Кр. Л., Коновалова С. С., Титов С. С.	Дискретная математика: учебное пособие для занятий и самостоятельной работы студентов по дисциплине "Дискретная математика" направления подготовки 090900.62-"Информационная безопасность" очной формы обучения	Екатеринбург: УрГУПС, 2015	25	29	http://biblioserver.usurt.ru/cgi-bin/irbis64r_13/cgiirbis_64.exe?C21COM=F&I21DBN=KN&P21DBN=KN
8	Голицына, Попов, Максимов	Информационные системы: Учебное пособие	Москва: Издательство "ФОРУМ", 2014	-	29	http://znanium.com/go.php?id=435900
9	Коновалов Б. И., Лебедев Ю. М.	Теория автоматического управления	Москва: Лань", 2016	-	29	http://e.lanbook.com/books/element.php?pl1_id=71753
10	[Российская Федерация]	Трудовой кодекс Российской Федерации: текст с изменениями и дополнениями на 25 апреля 2013 г.	Москва: Эксмо, 2013	1	-	
11	Корниенко А. А.	Информационная безопасность и защита информации на железнодорожном транспорте: в 2-х ч. : рекомендовано Экспертным советом по рецензированию Моск. гос. ун-та путей сообщ. в качестве учебника для студентов, обучающихся по специальности 090302.65 "Информационная безопасность телекоммуникационных систем" ВПО	Москва: Учебно-методический центр по образованию на ж.-д. трансп., 2014	5	29	http://e.lanbook.com/books/element.php?pl1_id=59240

12		Гражданский кодекс Российской Федерации: [ч. 1, 2, 3, 4 : официальный текст : текст Кодекса приводится по состоянию на 23 мая 2014 г.]	Москва: ОМЕГА-Л, 2014	2	-	
13	Девянин П. Н.	Модели безопасности компьютерных систем. Управление доступом и информационными потоками: рекомендовано Государственным образовательным учреждением высшего профессионального образования «Академия Федеральной службы безопасности Российской Федерации» в качестве учебного пособия для студентов высших учебных заведений, обучающихся по специальностям направления подготовки 090300 - «Информационная безопасность вычислительных, автоматизированных и телекоммуникационных систем» и направлению подготовки 090900 - «Информационная безопасность».	Москва: Горячая линия - Телеком, 2013	-	29	http://e.lanbook.com/books/element.php?pl1_id=63235
14	Партыка, Попов	Операционные системы, среды и оболочки: Учебное пособие	Москва: Издательство "ФОРУМ", 2013	-	29	http://znanium.com/go.php?id=405821
15	Кузин А. В., Кузин Д. А.	Компьютерные сети: Учебное пособие	Москва: Издательство "ФОРУМ", 2016	-	29	http://znanium.com/go.php?id=536468
16	Паршин К. А.	Оценка уровня информационной безопасности на объекте информатизации	Москва: УМЦ ЖДТ (Учебно-методический центр по образованию на железнодорожном	-	29	http://e.lanbook.com/books/element.php?pl1_id=80018
17	Милославская Н. Г.	"Серия «Вопросы управление информационной безопасностью"". Выпуск 3"	Москва: Горячая линия-Телеком, 2013	-	29	http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=5180
18	Бухтояров, Золотарев, Жуков	Поддержка принятия решений при проектировании систем защиты информации: Монография	Москва: ООО "Научно-издательский центр ИНФРА-М", 2014	-	29	http://znanium.com/go.php?id=445551
19	Козлов А. Ю., Мхитарян В. С., Шишов В. Ф.	Статистический анализ данных в MS Excel: Учебное пособие	Москва: ООО "Научно-издательский центр ИНФРА-М", 2016	-	29	http://znanium.com/go.php?id=558444

20	Лемешко Б. Ю., Постовалов С. Н., Лемешко С. Б., Чимитова Е. В.	Статистический анализ данных, моделирование и исследование вероятностных закономерностей. Компьютерный подход	Москва: ООО "Научно-издательский центр ИНФРА-М", 2015	-	29	http://znanium.com/go.php?id=515227
21	Вуколов	Основы статистического анализа. Практикум по статистическим методам и исследованию операций с использованием пакетов STATISTICA и EXCEL: Учебное пособие	Москва: Издательство "ФОРУМ", 2013	-	29	http://znanium.com/go.php?id=369689
22	Глазырин Г. В.	Теория автоматического регулирования	Новосибирск: Новосибирский государственный технический университет (НГТУ),	-	29	http://znanium.com/go.php?id=558731
23	Ездаков А. Л.	Экспертные системы САПР: Учебное пособие	Москва: Издательский Дом "ФОРУМ", 2016	-	29	http://znanium.com/go.php?id=518395
24	Кабашов	Электронное правительство. Электронный документооборот. Термины и определения: Учебное пособие	Москва: ООО "Научно-издательский центр ИНФРА-М", 2013	-	29	http://znanium.com/go.php?id=410730
25	Карпова И. П.	Базы данных: курс лекций и материалы для практических занятий : издание соответствует программе курса "Базы данных" по специальности 230101 "Вычислительные машины, комплексы, системы и сети" и может быть рекомендовано в качестве учебного пособия для студентов технических факультетов, изучающих автоматизированные информационные системы и системы управления базами данных	Санкт-Петербург: Питер, 2013	1	-	

26	Олифер В. Г., Олифер Н. А.	Компьютерные сети: принципы, технологии, протоколы : рекомендовано Министерством образования и науки РФ в качестве учебного пособия для студентов вузов, обучающихся по направлению "Информатика и и вычислительная техника" и по специальностям "Вычислительные машины, комплексы, системы и сети", "Автоматизированные машины, комплексы, системы и сети", "Программное обеспечение вычислительной техники и автоматизированных систем"	Санкт-Петербург: Питер, 2015	20	-	
27	Таненбаум Э.	Современные операционные системы	Санкт-Петербург: Питер, 2015	20	-	
28	Партыка Т. Л., Попов И. И.	Информационная безопасность: Учебное пособие	Москва: Издательство "ФОРУМ", 2016	-	29	http://znanium.com/go.php?id=516806
29	Паршин К. А.	Оценка уровня информационной безопасности на объекте информатизации: допущено Федеральным агентством железнодорожного транспорта в качестве учебного пособия для студентов вузов железнодорожного транспорта	Москва: ФГБОУ "Учеб.-метод. центр по образованию на ж.-д. трансп.", 2015	10	-	
30	Козлов, Мхитарян, Шишов	Статистический анализ данных в MS Excel: Учебное пособие	Москва: Издательский Дом "ИНФРА-М", 2014	-	29	http://znanium.com/go.php?id=429722
31	Мартишин С. А., Симонов В. Л., Храпченко М. В.	Базы данных.Практическое применение СУБД SQL и NoSOL-типа для применения проектирования информационных систем: Учебное пособие	Москва: Издательский Дом "ФОРУМ", 2017	-	29	http://znanium.com/go.php?id=556449
32	Васюткина И. А., Трошина Г. В., Бычков М. И., Менжулин С.	Разработка приложений на C# с использованием СУБД PostgreSQL	Новосибирск: Новосибирский государственный технический университет (НГТУ),	-	29	http://znanium.com/go.php?id=556925

33	Мартишин, Симонов, Храпченко	Проектирование и реализация баз данных в СУБД MySQL с использованием MySQL Workbench: Методы и средства проектирования информационных систем и технологий. Инструментальные средства информационных систем. Учебное пособие	Москва: Издательский Дом "ФОРУМ", 2012	-	29	http://znanium.com/go.php?id=318518
34	Култыгин О. П.	Администрирование баз данных. СУБД MS SQL Server	Москва: Московская финансово-промышленная академия (МФПА), 2012	-	29	http://znanium.com/go.php?id=451114
35	Гобарева Я. Л., Золотарюк А. В., Городецкая О. Ю.	Бизнес-аналитика средствами Excel: Учебное пособие	Москва: Вузовский учебник, 2017	-	29	http://znanium.com/go.php?id=636239
36	Гобарева Я. Л., Золотарюк А. В., Городецкая О. Ю.	Бизнес-аналитика средствами Excel: Учебное пособие	Москва: Вузовский учебник, 2015	-	29	http://znanium.com/go.php?id=478466

Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Кол-во. экз.	Кол-во. точек	Web-ссылка
1	Зубков А.М., Севастьянов Б.А., Чистяков В.П.	Сборник задач по теории вероятностей: Учеб. пособие для студентов вузов	Москва: Наука, Главная редакция физико-математической литературы, 1989	2	-	
2	Акулич И. Л.	Математическое программирование в примерах и задачах: учеб. пособие	Москва: Лань, 2011	-	29	http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=2027
3	Фишбейн Л. А.	Применение физических эффектов в технике: в 2-х частях : конспект лекций для студентов-бакалавров направления подготовки 15.03.06 - "Мехатроника и робототехника" всех форм обучения	Екатеринбург: УрГУПС, 2016	-	29	http://biblioserver.usurt.ru/cgi-bin/irbis64r_13/cgiirbis_64.exe?C21COM=F&I21DBN=KN&P21DBN=KN
4	Шейдаков Н. Е., Тищенко Е. Н., Серпенинов О. В.	Физические основы защиты информации: Учебное пособие	Москва: Издательский Центр РИО, 2016	-	29	http://znanium.com/go.php?id=556661
5	Гусев В. А., Мордкович А. Г.	Справочник по математике	Москва: Просвещение, 1995	1	-	

6	Гончарь П. С., Гончарь Л. Э., Завалищин Д. С.	Теория игр: учебное пособие для студентов, бакалавров и магистрантов экономических специальностей	Екатеринбург: УрГУПС, 2011	42	29	http://biblioserver.usurt.ru/cgi-bin/irbis64r_13/cgiirbis_64.e
7	Дьяконов В.	Mathcad 2001: Учеб. курс	СПб.: Питер, 2001	2	-	
8	Соколов Г.А., Чистякова Н.А.	Теория вероятностей: Учебник для студентов, обучающихся по направлению экономики	Москва: Экзамен, 2005	1	-	
9	Глухов М. М., Круглов И. А., Пичкур А. Б., Черемушкин А. В.	Введение в теоретико-числовые методы криптографии: учебное пособие : допущено УМО вузов по образованию в области информационной безопасности в качестве учебного пособия для студентов высших учебных заведений, обучающихся по специальности «Криптография»	Санкт-Петербург: Лань, 2011	-	29	http://e.lanbook.com/books/element.php?pl1_id=68466
10	Востриков А.С., Французова Г.А.	Теория автоматического регулирования: Учебное пособие для вузов по направлению "Автоматизация и управление"	Москва: Высшая школа, 2004	10	-	
11	Бесекерский В. А., Попов Е. П.	Теория систем автоматического управления: [учебное пособие]	СПб.: Профессия, 2007	48	-	
12	Стрельцов А. А.	Организационно-правовое обеспечение информационной безопасности: учебное пособие для студентов вузов, обучающихся по специальностям 090102 "Компьютерная безопасность", 090105 "Комплексное обеспечение информационной безопасности автоматизированных систем", 090106 "Информационная безопасность телекоммуникационных систем"	Москва: Академия, 2008	15	-	
13	Щербаков А. Ю.	Современная компьютерная безопасность: теоретические основы : практические аспекты : рек. М-вом образования и науки РФ в качестве учебного пособия для студентов вузов	Москва: Книжный мир, 2009	1	-	

14	Таненбаум Э.	Архитектура компьютера: [пер. с англ.]	СПб. [и др.]: Питер, 2012	40	-	
15	Карпова И. П.	Базы данных: курс лекций и материалы для практических занятий : издание соответствует программе курса "Базы данных" по специальности 230101 "Вычислительные машины, комплексы, системы и сети" и может быть рекомендовано в качестве учебного пособия для студентов технических факультетов, изучающих автоматизированные информационные системы и системы управления базами данных	Санкт-Петербург: Питер, 2013	1	-	
16	Хорев П. Б.	Методы и средства защиты информации в компьютерных системах: учебное пособие для студентов вузов, обучающихся по направлению 230100- "Информатика и вычислительная техника"	Москва: Академия, 2008	31	-	
17	Олифер В.Г., Олифер Н.А.	Сетевые операционные системы: учебник для студентов вузов, обучающихся по специальности "Информатика и вычислительная техника"	СПб.: Питер, 2008	2	-	
18	Олифер В.Г., Олифер Н.А.	Компьютерные сети. Принципы, технологии, протоколы: Учебное пособие для студентов вузов, обучающихся по специальностям 220100- "Вычислительные машины, комплексы, системы и сети", 220200- "Автоматизированные системы обработки информации и управления", 220400- "Программное обеспечение вычислительной техники и автоматизированных систем"	СПб.: Питер, 2008	14	-	
19	Таненбаум Э., Вудхалл А.	Операционные системы. Разработка и реализация: [пер. с англ.]	СПб.: Питер, 2007	1	-	
20	Галатенко В.А., Бетелин В.Б.	Основы информационной безопасности. Курс лекций: Учебное пособие для студентов вузов, обучающихся по	Москва: ИНТУИТ.РУ, 2006	1	-	

21	Куприянов А. И., Сахаров А. В., Шевцов В. А.	Основы защиты информации: учебное пособие для студентов вузов, обучающихся по специальностям "Радиоэлектронные системы", "Средства радиоэлектронной борьбы", "Информационные системы и технологии"	Москва: Академия, 2008	15	-	
22	Зырянова Т. Ю., Захарова А. А., Ялышев Ю. И.	Управление информационными рисками: монография	Тюмень: Издательство Тюменского гос. ун-та : Виндекс, 2008	10	-	
23	Репин В. В., Елиферов В. Г.	Процессный подход к управлению. Моделирование бизнес-процессов	Москва: Стандарты и качество, 2009	3	-	
24	Петренко С. А., Симонов С. В.	Управление информационными рисками: экономически оправданная безопасность : информационные технологии для инженеров	Москва: ДМК Пресс, 2009	-	29	http://e.lanbook.com/books/element.php?pl1_id=40021
25	Золотарев	Управление информационной безопасностью. Ч. 1. Анализ информационных рисков	Красноярск: Сибирский государственный аэрокосмический университет имени	-	29	http://znanium.com/go.php?id=463037
26	Жукова	Управление информационной безопасностью. Ч. 2. Управление инцидентами информационной безопасности	Красноярск: Сибирский государственный аэрокосмический университет имени	-	29	http://znanium.com/go.php?id=463061
27	Петровский А. Б.	Теория принятия решений: учебник для студентов вузов, обучающихся по специальности "Автоматизированные системы обработки информации и управления"	Москва: Академия, 2009	50	-	
28	Дорогов, Теплова	Введение в методы и алгоритмы принятия решений: Учебное пособие	Москва: Издательский Дом "ФОРУМ", 2012	-	29	http://znanium.com/go.php?id=241287
29	Воскобойников Ю.Е.	Регрессионный анализ данных в пакете Mathcad: учеб. пособие	Москва: Лань, 2011	-	29	http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=666
30	Барский А.Б.	Логические нейронные сети: учебное пособие	Москва: ИНТУИТ.РУ, 2007	5	-	
31	Хайкин С.	Нейронные сети: полный курс: научно-популярная литература	Москва: Вильямс, 2006	5	-	

32	Боровиков В.	Statistica: Искусство анализа данных на компьютере: Для профессионалов	СПб.: Питер, 2001	1	-	
33	Бесекерский В. А., Герасимов А. Н., Лучко С. В., Небылов А. В., Порфирьев Л. Ф., Фабрикант Е. А., Федоров С. М., Цветков В. И., Бесекерский В. А.	Сборник задач по теории автоматического регулирования и управления: доп. М-вом высшего и среднего спец. образования СССР в качестве учебного пособия для студентов вузов	Москва: Наука, Главная редакция физико-математической литературы, 1978	2	-	
34	Подобед М.А.	Документооборот предприятия	Москва: ПРИОР-издат, 2002	2	-	
35	Чукалова Л.Г.	Защита и обработка конфиденциальных документов: Курс лекций для студентов специальности 090103-"Организация и технология защиты информации"	Екатеринбург, 2005	26	29	http://biblioserver.usurt.ru/cgi-bin/irbis64r_13/cgiirbis_64.exe?C21COM=F&I21DBN=K
36	Бардаев Э. А., Кравченко В. Б.	Документоведение: учебник для студентов вузов, обучающихся по специальностям "Организация и технология защиты информации" и "Комплексная защита объектов информатизации" направления подготовки "Информационная безопасность"	Москва: Академия, 2010	15	-	
37	Романов О. А., Бабин С. А., Жданов С. Г.	Организационное обеспечение информационной безопасности: учебник для студентов вузов, обучающихся по специальностям "Организация и технология защиты информации", "Комплексная защита объектов информации"	Москва: Академия, 2008	15	-	
38	Шаталова Н. И.	Закономерности и особенности организационной системы предприятия	Екатеринбург: УрГУПС, 2010	-	29	http://biblioserver.usurt.ru/cgi-bin/irbis64r_13/cgiirbis_64.e

39	Бакланов В. В., Гайдамакин Н. А.	Защитные механизмы операционной системы Linux: допущено УМО по образованию в области информационной безопасности в качестве учебного пособия для студентов, обучающихся по специальностям "Компьютерная безопасность" и "Комплексное обеспечение информационной безопасности автоматизированных систем"	Екатеринбург: УрФУ, 2012	1	-	
40	Козлов, Мхитарян, Шишов	Статистический анализ данных в MS Excel: Учебное пособие	Москва: Издательский Дом "ИНФРА-М", 2012	-	29	http://znanium.com/go.php?id=238654
41	Урман С.	Oracle 8i: Новые возможности программирования на языке PL/SQL	Москва: Лори, 2001	1	-	

Методические разработки

	Авторы, составители	Заглавие	Издательство, год	Кол-во. экз.	Кол-во. точек	Web-ссылка
1	Гниломедов П. И., Пирогова И. Н., Скачков П. П.	Математическое моделирование: учебно-методическое пособие для занятий и самостоятельной работы студентов заочной формы обучения	Екатеринбург: УрГУПС, 2012	30	29	http://biblioserver.usurt.ru/cgi-bin/irbis64r_13/cgiirbis_64.exe?C21COM=F&I21DBN=K
2	Гончарь П. С., Гончарь Л. Э., Завалищин Д. С.	Задания по теории игр с примерами решения: учебно-методическое пособие для студентов экономических специальностей и направлений подготовки	Екатеринбург: УрГУПС, 2012	36	29	http://biblioserver.usurt.ru/cgi-bin/irbis64r_13/cgiirbis_64.exe?C21COM=F&I21DBN=KN&P21DBN=
3	Замыслов В. Е., Мезенцев А. В., Скачков П. П.	Численные методы: методические рекомендации к выполнению типового расчета для студентов специальности 190401.65 - "Эксплуатация ж. д."	Екатеринбург: УрГУПС, 2013	15	29	http://biblioserver.usurt.ru/cgi-bin/irbis64r_13/cgiirbis_64.exe?C21COM=
4	Замыслов В. Е.	Компьютерная обработка результатов наблюдений: методические указания к расчетно-графическим работам для студентов всех специальностей дневной и заочной форм обучения	Екатеринбург: УрГУПС, 2015	-	29	http://biblioserver.usurt.ru/cgi-bin/irbis64r_13/cgiirbis_64.exe?C21COM=F&I21DBN=KN&P21DBN=

5	Гончарь П. С., Гончарь Л. Э., Белослудцев О. А.	Сетевые модели в управлении проектами: учебное пособие для студентов экономических и управленческих направлений подготовки бакалавров: 080100.62 - "Экономика", 080200.62 - "Менеджмент", 080400.62 - "Управление персоналом", 100700.62 - "Торговое дело" всех форм обучения	Екатеринбург: УрГУПС, 2014	25	29	http://biblioserver.usurt.ru/cgi-bin/irbis64r_13/cgiirbis_64.exe?C21COM=F&I21DBN=KN&P21DBN=KN
6	Коновалова С. С., Титов С. С.	Дискретная математика: сборник контрольных заданий для студентов заочной формы обучения специальности 230201- "Информационные системы и технологии"	Екатеринбург: УрГУПС, 2010	30	29	http://biblioserver.usurt.ru/cgi-bin/irbis64r_13/cgiirbis_64.exe?C21COM=F&I21DBN=KN&P21DBN=KN
7	Баранов В. А., Нестеров В. Л., Ракина Н. Л.	Системы автоматического управления: учебно-методическое пособие по курсовому проектированию по дисциплине "Теория автоматического управления" для студентов специальности 190901 - "Системы обеспечения движения поездов" всех форм обучения	Екатеринбург: УрГУПС, 2013	22	29	http://biblioserver.usurt.ru/cgi-bin/irbis64r_13/cgiirbis_64.exe?C21COM=F&I21DBN=KN&P21DBN=KN
8	Чукалова Л.Г.	Защита и обработка конфиденциальных документов: Курс лекций для студентов специальности 090103-"Организация и технология защиты информации"	Екатеринбург, 2005	26	29	http://biblioserver.usurt.ru/cgi-bin/irbis64r_13/cgiirbis_64.exe?C21COM=F&I21DBN=KN&P21DBN=KN
9	Чукалова Л. Г.	Подготовка и обработка конфиденциальных документов: методические рекомендации к выполнению контрольной работы для студентов 4 курса специальности - 090103 - "Организация и технология защиты информации" дневной формы обучения	Екатеринбург: УрГУПС, 2011	-	29	http://biblioserver.usurt.ru/cgi-bin/irbis64r_13/cgiirbis_64.exe?C21COM=F&I21DBN=KN&P21DBN=KN
10	Паршин К. А.	Информационная безопасность и защита информации: методические указания по выполнению курсовой работы для студентов всех форм обучения специальности 071900- "Информационные системы и технологии"	Екатеринбург: УрГУПС, 2010	20	29	http://biblioserver.usurt.ru/cgi-bin/irbis64r_13/cgiirbis_64.exe?C21COM=F&I21DBN=KN&P21DBN=KN
11	Коллеров А. С., Корольков Ю. Д., Синадский Н. И., Соболев	Основы информационной безопасности: учебное пособие	Иркутск: Издательство ИГУ, 2013	1	-	

12	Сурин А. В., Окулов Н. Е.	Информационные технологии на транспорте: практикум для студентов спец. 190701 - "Организация перевозок и упр. на трансп. (ж.-д. трансп.)"	Екатеринбург: УрГУПС, 2012	49	29	http://biblioserver.usurt.ru/cgi-bin/irbis64r_13/cgiirbis_64.exe?C21COM=F&I21DBN=KN&P21DBN=KN
13	Духан Е. И., Корольков Ю. Д., Синадский Н. И.	Средства защиты информации от несанкционированного доступа: учебное пособие	Иркутск: Издательство ИГУ, 2012	1	-	
14	Духан Е. И., Корольков Ю. Д., Синадский Н. И.	Средства криптографической защиты компьютерной информации: учебное пособие	Иркутск: Издательство ИГУ, 2012	1	-	
15	Борисенко М. Л., Дудоров Е. Н., Корольков Ю. Д.	Защита информации в операционных системах MS Windows: учебное пособие	Иркутск: Издательство ИГУ, 2012	1	-	
16	Мезенцев А. В., Синадский Н. И., Хорьков Д. А.	Технологии защищенной обработки информации	Иркутск: Издательство ИГУ, 2013	1	-	
17	Коллеров А. С., Корольков Ю. Д., Синадский Н. И., Хорьков	Системы обнаружения компьютерных атак: учебное пособие	Иркутск: Издательство ИГУ, 2013	1	-	
18	Андрончик А. Н., Иванов Ф. И., Щербаков М. Ю.	Мониторинг и управление в компьютерных сетях: учебное пособие	Иркутск: Издательство ИГУ, 2013	1	-	
19	Агафонов А. В., Андрончик А. Н., Корольков Ю. Д.	Технологии межсетевого экранирования: учебное пособие	Иркутск: Издательство ИГУ, 2013	1	-	
20	Корольков Ю. Д., Синадский Н. И.	Анализ и восстановление данных в операционных системах MS Windows: учебное пособие	Иркутск: Издательство ИГУ, 2012	1	-	
21	Корольков Ю. Д., Синадский Н. И., Хорьков Д. А.	Аудит информационной безопасности компьютерных систем: учебное пособие	Иркутск: Издательство ИГУ, 2012	1	-	
22	Ковалев И. А., Пермикин В. Ю., Шипулин А. В., Сурин А. В.	Теория принятия решений: учебно-методическое пособие по проведению практических занятий для студентов вузов очной и заочной форм обучения	Екатеринбург: УрГУПС, 2009	65	29	http://biblioserver.usurt.ru/cgi-bin/irbis64r_13/cgiirbis_64.exe?C21COM=F&I21DBN=KN&P21DBN=KN

23	Тарасян В. С.	Основы теории нечетких множеств: учебное пособие по курсу "Методы искусственного интеллекта" для студентов специальности 220401 - "Мехатроника" направления 220400 - "Мехатроника и робототехника"	Екатеринбург: УрГУПС, 2012	27	29	http://biblioserver.usurt.ru/cgi-bin/irbis64r_13/cgiirbis_64.exe?C21COM=F&I21DBN=KN&P21DBN=KN
24	Тарасян В. С.	Пакет Fuzzy Logic Toolbox For Matlab: учебное пособие по курсу "Методы искусственного интеллекта" для студентов специальности 220401 - "Мехатроника" направления 220400 - "Мехатроника и робототехника"	Екатеринбург: УрГУПС, 2013	26	29	http://biblioserver.usurt.ru/cgi-bin/irbis64r_13/cgiirbis_64.exe?C21COM=F&I21DBN=KN&P21DBN=KN
25	Паршин К. А., Копылова А. А.	Технология защиты речевой информации в помещениях: учебно-методическое пособие по выполнению курсовой работы для студентов очной формы обучения специальности 090103- "Организация и технология защиты информации"	Екатеринбург: УрГУПС, 2010	17	29	http://biblioserver.usurt.ru/cgi-bin/irbis64r_13/cgiirbis_64.exe?C21COM=F&I21DBN=KN&P21DBN=KN
26	Паршин К. А.	Технологии обработки информации на объекте защиты: учебно-методическое пособие для студентов очной формы обучения специальности 090103- "Организация и технология защиты информации и студентов всех форм обучения специальности 071900- "Информационные системы и технологии"	Екатеринбург: УрГУПС, 2010	30	29	http://biblioserver.usurt.ru/cgi-bin/irbis64r_13/cgiirbis_64.exe?C21COM=F&I21DBN=KN&P21DBN=KN

5.6 Методические материалы, определяющие процедуру оценивания результатов освоения образовательной программы

Итоговая оценка за выполнение и защиту ВКР складывается из оценок сформированности компетенций, продемонстрированных выпускником при выполнении и защите ВКР и оценок общих критериев оценивания ВКР:

- хода подготовки ВКР – оценивает руководитель, консультанты по экономическому разделу и разделу «Безопасность жизнедеятельности»;
- текста ВКР – оценивают руководитель, консультанты по экономическому разделу и разделу «Безопасность жизнедеятельности», рецензент (при наличии);
- доклада на защите и презентации работы – оценивают члены ГЭК;
- ответов на вопросы членов ГЭК – оценивают члены ГЭК.

Таблица 5 – Результаты освоения ОП ВО (ВКР)

Код компе-тенции	Компоненты, подлежащие оцениванию	Результаты освоения ОП ВО (ВКР)	Лица, оценивающие сформирован-ность компетенций
1	2	3	4
Общекультурные			
ОК-1	Текст ВКР	*Знать*: приемы философского анализа проблем. *Уметь*: анализировать проблемы и планировать свою деятельность с учетом результатов этого анализа. *Владеть*: навыками публичной речи, аргументации, ведения дискуссии и полемики, навыками письменного аргументированного изложения собственной точки зрения	Руководитель, рецензент
	Ответы на вопросы членов ГЭК		Члены ГЭК
ОК-2	Текст ВКР	*Знать*: основные понятия экономической деятельности в области защиты информации. *Уметь*: оценивать эффективность и анализировать экономические показатели в области защиты информации. *Владеть*: навыками экономического обоснования выбранного решения.	Руководитель, рецензент, консультант
	Доклад на защите и презентация работы		Члены ГЭК
	Ответы на вопросы членов ГЭК		Члены ГЭК
ОК-3	Текст ВКР	*Знать:* основные исторические аспекты развития системы защиты информации. *Уметь*: осуществлять эффективный поиск информации и критику источников. *Владеть*: приемами ведения дискуссии и полемики.	Руководитель, рецензент
	Доклад на защите и презентация работы		Члены ГЭК
	Ответы на вопросы членов ГЭК		Члены ГЭК
ОК-4	Текст ВКР	*Знать:* законодательство в области защиты информации. *Уметь*: использовать в практической деятельности правовые знания. *Владеть*: навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности.	Руководитель, рецензент
	Доклад на защите и презентация работы		Члены ГЭК
	Ответы на вопросы членов ГЭК		Члены ГЭК

Код компе-тенции	Компоненты, подлежащие оцениванию	Результаты освоения ОП ВО (ВКР)	Лица, оценивающие сформирован-ность компетенций
1	2	3	4
ОК-5	Текст ВКР	*Знать:* основы российской правовой системы в области защиты информации, характеристики организации деятельности органов государственной власти в Российской Федерации, правовые основы обеспечения национальной безопасности Российской Федерации. *Уметь*: формулировать и аргументировано отстаивать собственную позицию по различным проблемам с соблюдением норм профессиональной этики. *Владеть*: приемами ведения дискуссии и полемики с соблюдением норм профессиональной этики.	Руководитель, рецензент
	Доклад на защите и презентация работы		Члены ГЭК
	Ответы на вопросы членов ГЭК		Члены ГЭК
ОК-6	Ход подготовки ВКР	*Знать*: основные понятия и методы в области управленческой деятельности. *Уметь*: осуществлять планирование и организацию работы коллектива при выполнении поставленных задач. *Владеть*: навыками обоснования, реализации и контроля результатов управленческих решений по организации работы коллектива.	Руководитель
ОК-7	Текст ВКР	*Знать*: иностранный язык в объеме, необходимом для получения профессиональной информации из зарубежных источников и общения на деловом уровне; профессиональную лексику иностранного языка в объеме, необходимом для общения, чтения и перевода иноязычных текстов в рамках делового общения в профессиональной деятельности; основные грамматические явления и структуры государственного (русского) языка, используемые в устном и письменном общении в профессиональной деятельности. *Уметь*: использовать иностранный язык в межличностном общении и профессиональной деятельности; соблюдать речевой этикет в ситуациях повседневного и делового общения (устанавливать и поддерживать контакты, завершить беседу, запрашивать и сообщать информацию). *Владеть*: основами публичной речи, перевода текстов по специальности; навыками грамотно и эффективно пользоваться источниками информации (справочной литературой, ресурсами Интернет); навыками выражения своего мнения в процессе делового общения на иностранном языке.	Руководитель, рецензент
	Доклад на защите и презентация работы		Члены ГЭК
	Ответы на вопросы членов ГЭК		Члены ГЭК

Код компе-тенции	Компоненты, подлежащие оцениванию	Результаты освоения ОП ВО (ВКР)	Лица, оценивающие сформирован-ность компетенций
1	2	3	4
ОК-8	Ход подготовки ВКР	*Знать*: методы самоорганизации и самообразования, планирования своей деятельности. *Уметь*: осуществлять планирование и организацию собственной деятельности, осуществлять эффективный поиск информации. *Владеть*: навыками обоснования, реализации и контроля собственной деятельности, навыками систематизации и анализа информации.	Руководитель
ОК-9	Ход подготовки ВКР	*Знать*: роль и значение физической культуры в системе научной организации труда, влияние условий и характера труда на выбор форм, методов и средств производственной физической культуры. *Уметь*: интегрировать полученные знания в формирование профессионально значимых умений и навыков. *Владеть*: средствами и методами укрепления индивидуального здоровья, физического самосовершенствования для успешной социально-культурной и профессиональной деятельности; методиками и методами самодиагностики, самооценки, средствами оздоровления для самокоррекции здоровья различными формами двигательной деятельности, удовлетворяющими потребности человека в рациональном использовании свободного времени.	Руководитель
	Доклад на защите и презентация работы		Члены ГЭК
Общепрофессиональные			
ОПК-1	Текст ВКР	*Знать*: особенности физических эффектов и явлений, используемые для обеспечения информационной безопасности. *Уметь*: применять основные законы физики при решении практических задач. *Владеть*: навыками проведения физического эксперимента и обработки его результатов.	Руководитель, рецензент
	Доклад на защите и презентация работы		Члены ГЭК
	Ответы на вопросы членов ГЭК		Члены ГЭК
ОПК-2	Текст ВКР	*Знать*: основные методы решения задач профессиональной области и применением математических методов и моделей. *Уметь*: использовать математические методы и модели для решения прикладных задач. *Владеть*: навыками применения математического аппарата для решения прикладных задач в области защиты информации.	Руководитель, рецензент
	Доклад на защите и презентация работы		Члены ГЭК
	Ответы на вопросы		Члены ГЭК

Код компе-тенции	Компоненты, подлежащие оцениванию	Результаты освоения ОП ВО (ВКР)	Лица, оценивающие сформирован-ность компетенций
1	2	3	4
	членов ГЭК		
ОПК-3	Текст ВКР	*Знать*: принципы работы современной радиоэлектронной аппаратуры и физические процессы, протекающие в них. *Уметь*: применять полученные знания при использовании механизмов и приборов. *Владеть*: навыками работы с основными измерительными приборами.	Руководитель, рецензент
	Доклад на защите и презентация работы		Члены ГЭК
	Ответы на вопросы членов ГЭК		Члены ГЭК
ОПК-4	Текст ВКР	*Знать*: основные понятия информатики. *Уметь*: использовать программные и аппаратные средства современного компьютера. *Владеть*: навыками поиска информации в глобальной сети Интернет и работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов).	Руководитель, рецензент
	Доклад на защите и презентация работы		Члены ГЭК
	Ответы на вопросы членов ГЭК		Члены ГЭК
ОПК-5	Текст ВКР	*Знать*: правовые основы обеспечения информационной безопасности. *Уметь*: применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности. *Владеть*: навыками работы с нормативными правовыми актами.	Руководитель, рецензент
	Доклад на защите и презентация работы		Члены ГЭК
	Ответы на вопросы членов ГЭК		Члены ГЭК
ОПК-6	Текст ВКР	*Знать*: опасные и вредные факторы системы «человек – среда обитания», методы анализа антропогенных опасностей. *Уметь*: анализировать и оценивать степень риска проявления факторов опасности системы «человек – среда обитания», осуществлять и контролировать выполнения требований по охране труда и безопасности жизнедеятельности. *Владеть*: навыками безопасного использования технических средств в профессиональной деятельности.	Руководитель, консультанты, рецензент
	Доклад на защите и презентация работы		Члены ГЭК
	Ответы на вопросы членов ГЭК		Члены ГЭК
ОПК-7	Текст ВКР	*Знать*: основные угрозы безопасности информации и модели нарушителя в информационных системах. *Уметь*: определять комплекс мер (правила, процедуры, практические приемы, руководящие методы, принципы, средства) для обеспечения информационной безопасности информационных систем.	Руководитель, рецензент
	Доклад на защите и презентация работы		Члены ГЭК
	Ответы на вопросы		Члены ГЭК

Код компе-тенции	Компоненты, подлежащие оцениванию	Результаты освоения ОП ВО (ВКР)	Лица, оценивающие сформирован-ность компетенций
1	2	3	4
	членов ГЭК	*Владеть*: навыками формальной постановки и решения задачи обеспечения информационной безопасности, навыками анализа информационной инфраструктуры информационной системы и ее безопасности.	
Профессиональные компетенции, соответствующие видам профессиональной деятельности, на которые ориентирована программа магистратуры: а) в эксплуатационной деятельности:			
ПК-1	Текст ВКР	*Знать*: принципы организации информационных систем в соответствии с требованиями по защите информации. *Уметь*: анализировать и оценивать угрозы информационно безопасности объектов, использовать программные и аппаратные средства современного компьютера. *Владеть*: методами установки и настройки программно-аппаратных и технических средств защиты информации.	Руководитель, рецензент
	Доклад на защите и презентация работы		Члены ГЭК
	Ответы на вопросы членов ГЭК		Члены ГЭК
ПК-2	Текст ВКР	*Знать*: принципы организации информационных систем в соответствии с требованиями по защите информации. *Уметь*: осуществлять меры противодействия нарушениям информационной безопасности. *Владеть*: профессиональной терминологией, навыками использования программных средств системного, прикладного и специального назначения.	Руководитель, рецензент
	Доклад на защите и презентация работы		Члены ГЭК
	Ответы на вопросы членов ГЭК		Члены ГЭК
ПК-3	Текст ВКР	*Знать*: принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации. *Уметь*: осуществлять меры противодействия нарушениям безопасности. *Владеть*: методикой анализа угроз безопасности информации.	Руководитель, рецензент
	Доклад на защите и презентация работы		Члены ГЭК
	Ответы на вопросы членов ГЭК		Члены ГЭК
ПК-4	Текст ВКР	*Знать*: принципы организации информационных систем в соответствии с требования по защите информации. *Уметь*: определять информационную инфраструктуру и информационные ресурса организации, подлежащие защите. *Владеть*: навыками анализа информационной инфраструктуры информационной системы и ее безопасности.	Руководитель, рецензент
	Доклад на защите и презентация работы		Члены ГЭК
	Ответы на вопросы членов ГЭК		Члены ГЭК
ПК-5	Текст ВКР	*Знать*: основные угрозы безопасности	Руководитель,

Код компе-тенции	Компоненты, подлежащие оцениванию	Результаты освоения ОП ВО (ВКР)	Лица, оценивающие сформирован-ность компетенций
1	2	3	4
		информации и модели нарушителя в информационных системах. *Уметь*: контролировать эффективность принятых мер по обеспечению информационной безопасности информационных систем. *Владеть*: навыками выбора и обоснования критериев эффективности функционирования защищенных информационных систем.	рецензент
	Доклад на защите и презентация работы		Члены ГЭК
	Ответы на вопросы членов ГЭК		Члены ГЭК
ПК-6	Текст ВКР	*Знать*: основные методы управления информационной безопасностью, принципы формирования политики безопасности в информационных системах. *Уметь*: определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите, разрабатывать модели угроз и нарушителей информационной безопасности. *Владеть*: навыками выбора и обоснования критериев эффективности функционирования защищенных информационных систем.	Руководитель, рецензент
	Доклад на защите и презентация работы		Члены ГЭК
	Ответы на вопросы членов ГЭК		Члены ГЭК
б) в проектно-технологической деятельности:			
ПК-7	Текст ВКР	*Знать*: современные угрозы безопасности информации и модели нарушителя в информационных системах. *Уметь*: разрабатывать модели угроз и нарушителей информационной безопасности информационных систем; выявлять уязвимости информационно-технологических ресурсов информационных систем, проводить мониторинг угроз безопасности информационных систем; оценивать информационные риски в информационных системах *Владеть*: методами мониторинга и аудита, выявления угроз информационной безопасности информационных систем; навыками выбора и обоснования критериев эффективности функционирования защищенных информационных систем.	Руководитель, рецензент
	Доклад на защите и презентация работы		Члены ГЭК
	Ответы на вопросы членов ГЭК		Члены ГЭК
ПК-8	Текст ВКР	*Знать*: теоретические основы документоведения, структуру документов и нормативные требования к их оформлению. *Уметь*: составлять документы на любом носителе в зависимости от содержания, назначения и вида документа. *Владеть*: навыками работы с документами.	Руководитель, рецензент
	Доклад на защите и презентация работы		Члены ГЭК
	Ответы на вопросы членов ГЭК		Члены ГЭК
в) в экспериментально-исследовательской деятельности:			

Код компетенции	Компоненты, подлежащие оцениванию	Результаты освоения ОП ВО (ВКР)	Лица, оценивающие сформированность компетенций
1	2	3	4
ПК-9	Текст ВКР	*Знать*: методы систематизации научно-технической информации, выбора методик и научных средств решения задач при решении прикладных проблем информационной безопасности. *Уметь*: разрабатывать планы и программы проведения научных исследований и технических разработок. *Владеть*: навыков сбора, обработки, анализа и систематизации научно-технической информации.	Руководитель, рецензент
	Доклад на защите и презентация работы		Члены ГЭК
	Ответы на вопросы членов ГЭК		Члены ГЭК
ПК-10	Текст ВКР	*Знать*: основные отечественные и международные стандарты информационной безопасности. *Уметь*: самостоятельно анализировать отечественные и международные стандарты информационной безопасности. *Владеть*: навыками применения отечественных и международных стандартов информационной безопасности.	Руководитель, рецензент
	Доклад на защите и презентация работы		Члены ГЭК
	Ответы на вопросы членов ГЭК		Члены ГЭК
ПК-11	Текст ВКР	*Знать*: основные понятия и методы математического анализа, теории вероятностей и математической статистики, основные понятия и методы математической логики и теории алгоритмов, дискретной математики; основные понятия, законы и модели электричества и магнетизма; основные понятия, законы и модели теории колебаний и волн, оптики, акустики; особенности физических эффектов и явлений, используемых для обеспечения информационной безопасности. *Уметь*: применять основные законы физики при решении практических задач; использовать математические методы и модели для решения прикладных задач; строить математические модели задач профессиональной области *Владеть*: навыками проведения физического эксперимента; методами количественного анализа процессов обработки, поиска и передачи информации	Руководитель, рецензент
	Доклад на защите и презентация работы		Члены ГЭК
	Ответы на вопросы членов ГЭК		Члены ГЭК
ПК-12	Текст ВКР	*Знать*: методологию создания систем защиты информации. *Уметь*: определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите. *Владеть*: методами мониторинга и аудита, выявления угроз информационной безопасности.	Руководитель, рецензент
	Доклад на защите и презентация работы		Члены ГЭК
	Ответы на вопросы		Члены ГЭК

Код компетенции	Компоненты, подлежащие оцениванию	Результаты освоения ОП ВО (ВКР)	Лица, оценивающие сформированность компетенций
1	2	3	4
	членов ГЭК		
г) в организационно-управленческой деятельности:			
ПК-13	Текст ВКР	*Знать*: основные методы управления информационной безопасностью *Уметь*: определять комплекс мер (правила, процедуры, практические приемы, руководящие методы, принципы, средства) для обеспечения информационной безопасности информационных систем. *Владеть*: методами управления информационной безопасностью информационных систем.	Руководитель, рецензент
	Доклад на защите и презентация работы		Члены ГЭК
	Ответы на вопросы членов ГЭК		Члены ГЭК
ПК-14	Ход работы над ВКР	*Знать*: основные понятия и методы в области управленческой деятельности; порядок выработки и реализации управленческих решений; состав системы управления и требования к ее элементам; содержание управленческой работы руководителя подразделения. *Уметь*: осуществлять планирование и организацию работы рабочего коллектива при выполнении поставленных задач; разрабатывать, реализовывать, оценивать и корректировать процессы управления информационной безопасностью. *Владеть*: навыками обоснования, выбора, реализации и контроля результатов управленческого решения	Руководитель
ПК-15	Текст ВКР	*Знать*: основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации; правовые основы организации защиты информации конфиденциального характера; организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения технической защиты информации конфиденциального характера, по аттестации объектов информатизации и сертификации средств защиты информации. *Уметь*: применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации. *Владеть*: навыками работы с нормативными правовыми актами; методами организации и управ-	Руководитель, рецензент
	Доклад на защите и презентация работы		Члены ГЭК
	Ответы на вопросы членов ГЭК		Члены ГЭК

Код компетенции	Компоненты, подлежащие оцениванию	Результаты освоения ОП ВО (ВКР)	Лица, оценивающие сформированность компетенций
1	2	3	4
		ления деятельностью служб защиты информации на предприятии; методами формирования требований по защите информации.	
Профессионально-специализированные компетенции			
ПСК-1	Текст ВКР	*Знать*: основы российской правовой системы в области защиты информации, основные понятия и методы в области управленческой деятельности, основные понятия экономической деятельности в области защиты информации. *Уметь*: определять комплекс мер (правила, процедуры, практические приемы, руководящие методы, принципы, средства) для обеспечения информационной безопасности информационных систем. *Владеть*: методами управления информационной безопасностью информационных систем.	Руководитель, рецензент
	Доклад на защите и презентация работы		Члены ГЭК
	Ответы на вопросы членов ГЭК		Члены ГЭК
ПСК-2	Текст ВКР	*Знать*: принципы организации информационных систем в соответствии с требованиями по защите информации. *Уметь*: определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; разрабатывать модели угроз и нарушителей информационной безопасности информационных систем; выявлять уязвимости информационно-технологических ресурсов информационных систем, проводить мониторинг угроз безопасности информационных систем. *Владеть*: методами управления информационной безопасностью информационных систем.	Руководитель, рецензент
	Доклад на защите и презентация работы		Члены ГЭК
	Ответы на вопросы членов ГЭК		Члены ГЭК
ПСК-3	Текст ВКР	*Знать*: этапы проектирования систем, комплексов, средства и технологий управления информационной безопасностью. *Уметь*: формировать требования к проектированию систем, комплексов, средства и технологий управления информационной безопасностью. *Владеть*: навыками разработки систем, комплексов, средства и технологий управления информационной безопасностью с учетом особенностей объектов защиты	Руководитель, рецензент
	Доклад на защите и презентация работы		Члены ГЭК
	Ответы на вопросы членов ГЭК		Члены ГЭК
ПСК-4	Текст ВКР	*Знать*: современные угрозы безопасности информации и модели нарушителя в информационных системах. *Уметь*: разрабатывать модели угроз и нарушителей информационной безопасности информационных систем; выявлять уязвимости информационно-технологических ресурсов информацион-	Руководитель, рецензент
	Доклад на защите и презентация работы		Члены ГЭК
	Ответы на		Члены ГЭК

Код компетенции	Компоненты, подлежащие оцениванию	Результаты освоения ОП ВО (ВКР)	Лица, оценивающие сформированность компетенций
1	2	3	4
	вопросы членов ГЭК	ных систем, проводить мониторинг угроз безопасности информационных систем; оценивать информационные риски в информационных системах *Владеть*: методами мониторинга и аудита, выявления угроз информационной безопасности информационных систем; навыками выбора и обоснования критериев эффективности функционирования защищенных информационных систем.	
ПСК-5	Текст ВКР	*Знать*: принципы организации информационных систем в соответствии с требованиями по защите информации. *Уметь*: определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; разрабатывать модели угроз и нарушителей информационной безопасности информационных систем; выявлять уязвимости информационно-технологических ресурсов информационных систем, проводить мониторинг угроз безопасности информационных систем. *Владеть*: методами управления информационной безопасностью информационных систем.	Руководитель, рецензент
	Доклад на защите и презентация работы		Члены ГЭК
	Ответы на вопросы членов ГЭК		Члены ГЭК
ПСК-6	Текст ВКР	*Знать*: принципы организации информационных систем в соответствии с требованиями по защите информации. *Уметь*: определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; разрабатывать модели угроз и нарушителей информационной безопасности информационных систем; выявлять уязвимости информационно-технологических ресурсов информационных систем, проводить мониторинг угроз безопасности информационных систем, определять комплекс мер (правила, процедуры, практические приемы, руководящие методы, принципы, средства) для обеспечения информационной безопасности информационных систем. *Владеть*: методами управления информационной безопасностью информационных систем.	Руководитель, рецензент
	Доклад на защите и презентация работы		Члены ГЭК
	Ответы на вопросы членов ГЭК		Члены ГЭК

Для оценки выпускной квалификационной работы применяется пятибалльная система оценки. Шкала и критерии оценивания компетенций представлены в таблице 3.

Кроме того, в качестве методических материалов, определяющих процедуру оценивания, используются положения:

ПЛ 2.3.23 – 2017 «Порядок проведения государственной итоговой аттестации по образовательным программам высшего образования – по программам бакалавриата, программам специалитета и программам магистратуры»;

СТО 2.3.5-2016 «Выпускная квалификационная работа: Требования к оформлению, порядок выполнения, критерии оценки»;

ПЛ 2.3.22–2014 «О формировании фонда оценочных средств».

6 Материально-техническое и программное обеспечение государственной итоговой аттестации

Для проведения ГИА используются аудитории университета, оборудованные средствами мультимедиа. При выполнении ВКР используется следующее материально-техническое и программное обеспечение (таблица 6).

Таблица 6 – Материально-техническое и программное обеспечение

Назначение аудитории/помещения	Оборудование	Приборы	Программно-аппаратные средства общего и специального назначения
Учебные аудитории для проведения занятий семинарского типа (практических занятий)	Персональные компьютеры, экран, проектор	–	Операционная система Windows Система электронной поддержки обучения Blackboard Learn (сайт bb.usurt.ru) Пакет офисных программ MS Office
Компьютерные классы	Персональные компьютеры	–	Операционная система Windows Система электронной поддержки обучения Blackboard Learn (сайт bb.usurt.ru) Пакет офисных программ MS Office Операционная система на базе ядра Linux – дистрибутив Debian Пакет прикладных программ Matlab/Simulink Система электронного документооборота Lotus Domino Пакет статистического

Назначение аудитории/помещения	Оборудование	Приборы	Программно-аппаратные средства общего и специального назначения
			анализа STATISTICA
Лаборатория «Технологии обеспечения информационной безопасности и техническая защита информации»	–	Система автоматизированная измерения действующих высот случайных антенн и коэффициентов реального затухания электромагнитных сигналов СТЕНТОР-М1 Анализатор спектра портативный R&S FSH 4/8 Анализатор спектра «GSP-810» Генератор сигналов AFG3110 Аппаратно-программный комплекс шифрования «Континент» Аппаратно-программный комплекс Oscor-50 Генератор шума «ГРОМ-ЗИ-4» Осциллограф цифровой GDS-820C Универсальный анализатор проводных линий ULAN-2 Комплекс для проведения акустических и виброакустических измерений «Спрут-7А» Анализатор качества электроэнергии в трехфазных сетях FLUKE 435 Детектор звукозаписывающих устройств Имитатор электростатических разрядов ЭСР-8000 К	–

Назначение аудитории/помещения	Оборудование	Приборы	Программно-аппаратные средства общего и специального назначения
		Источник питания регулированный MASTECH HY3020 Осциллограф цифровой Good Will instrument «GDS-71102A» Всенаправленный источник звука Bruel&Kjaer 4296 Шумомер-виброметр, анализатор спектра портативный ОКТАВА-110А с измерительными антеннами Индикатор поля D-008 Подавитель сотовой связи ЛГШ-718 Система защиты СОНАТА-АВ	
Лаборатория «Программно-аппаратные средства защищенных информационных систем»	Персональные компьютеры, экран, проектор	–	Система защиты информации ViPNet Операционная система специального назначения Astra Linux Special Edition Система защиты информации от несанкционированного доступа Secret Net Система защиты информации от несанкционированного доступа Страж NT Система защиты информации от несанкционированного доступа Dallas Lock

7 Информационные ресурсы, поисковые системы, базы данных

Таблица 7 – Информационные ресурсы

№п/п	Адрес в интернете, наименование, назначение
1	Информационный бюллетень «JetInfo On-line» (www.jetinfo.ru)
2	Журнал «Открытые системы» (www.osp.ru)
3	Журнал сетевых решений «LAN» (www.osp.ru/lan)
4	Журнал «Сети» (www.osp.ru/nets)

5	Журнал «Мир ПК» (www.osp.ru/pcworld)
6	Журнал «Инсайд. Защита информации» (http://www.inside-zi.ru/)
7	Журнал «Вестник УрФО. Безопасность в информационной сфере» (www.info-secur.ru)
8	Информационно-справочная система «Консультант-Плюс»

Лист согласования к программе государственной итоговой аттестации

Направление подготовки:
10.04.01 Информационная безопасность
(код и наименование направления подготовки)

Информационная безопасность на транспорте
(наименование направленности (профиля) образовательной программы)

Составитель _____ /Т.Ю. Зырянова/
(подпись) (Ф.И.О.)

Заведующий кафедрой
«Информационные технологии
и защита информации» _____ / Т.Ю. Зырянова/
(подпись) (Ф.И.О.)

Протокол заседания кафедры № 13 от «29» декабря 2016 г.

СОГЛАСОВАНО:

Начальник отдела ДиА _____ /Н.Ф. Сирина/
(подпись) (Ф.И.О.)

Председатель УМК факультета
(зам. председателя) _____ / Н.Л. Ракина /
(подпись) (Ф.И.О.)

Начальник учебного отдела _____ /М.Н. Оськина/
(подпись) (Ф.И.О.)