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

Кафедра *«Информационные технологии и защита информации»*

СОГЛАСОВАНО
Начальник отдела контроля и эксплуатации
средств защиты информации ЕИВЦ –
структурного подразделения ГВЦ –
филиала ОАО «РЖД»

_____ / С. А. Кикоть

Директор Екатеринбургского НТЦ ФГУП
«НПП «Гамма»

_____ / А. С. Худеньких

«01» сентября 2017г

УТВЕРЖДАЮ
Проректор по учебной работе
и связям с производством

_____ / Е. А. Малыгин

«01» сентября 2017г

ПРОГРАММА ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки

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

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

Квалификация
бакалавр

Форма обучения
очная

Екатеринбург 2017 г.

Оглавление

1 Общие положения ... 3

2 Структура государственной итоговой аттестации ... 3

3 Перечень планируемых результатов освоения образовательной программы (ОП) ... 3

4 Подготовка к сдаче и сдача государственного экзамена ... 13

4.1. Результаты освоения ОП ВО (ГИА) ... 14

4.2. Содержание государственного экзамена ... 18

4.3. Перечень вопросов, выносимых на государственный экзамен ... 21

4.4. Перечень рекомендуемой литературы для подготовки к государственному экзамену ... 24

4.5. Критерии оценки результатов сдачи государственного экзамена с описанием критериев оценивания компетенций, а также шкал оценивания ... 27

4.6. Методические материалы, определяющие процедуры оценивания результатов освоения образовательной программы на государственном экзамене ... 29

4.7. Рекомендации обучающимся по подготовке к государственному экзамену ... 30

5 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты ... 31

5.1 Требования к структуре, оформлению, порядку выполнения, критериям оценки, представлению к защите выпускной квалификационной работы ... 31

5.2 Процедура защиты ВКР, регламент работы государственной экзаменационной комиссии ... 31

5.3 Примерный перечень тем ВКР ... 31

5.4 Показатели и критерии оценивания компетенций, шкала оценивания ... 35

5.5 Перечень источников литературы при выполнении выпускной квалификационной работы ... 78

5.6 Методические материалы, определяющие процедуру оценивания результатов освоения образовательной программы ... 82

6 Материально-техническое и программное обеспечение государственной итоговой аттестации ... 92

7 Информационные ресурсы, поисковые системы, базы данных ... 92

ПРИЛОЖЕНИЕ 1 ... 94

1 Общие положения

Целью государственной итоговой аттестации является установление соответствия результатов освоения обучающимися образовательной программы 10.03.01 «Информационная безопасность» направленность (профиль) «Организация и технология защиты информации (на транспорте)», 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, завершающая 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 «СМК Порядок проведения государственной итоговой аттестации по образовательным программам высшего образования – по программам бакалавриата, программам специалитета и программам магистратуры».

2 Структура государственной итоговой аттестации

Государственная итоговая аттестация по данной образовательной программе включает:

- подготовку к сдаче и сдачу государственного экзамена;

- защиту выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты.

Государственная итоговая аттестация проводится согласно календарного учебного графика. Общий объем составляет 9 зачетных единиц (324 часа).

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», направленность (профиль) «Организация и технология защиты информации (на транспорте) (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	*Знать:* основы российской правовой системы в области защиты информации, характеристики организации деятельности органов государственной власти в Российской Федерации, правовые основы

Компетенция		Результаты освоения ОП ВО
Код	Содержание	
1	2	3
	мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	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.
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

Компетенция		Результаты освоения ОП ВО
Код	Содержание	
1	2	3
		систематизации и анализа информации.
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	*Знать*: правовые основы обеспечения

Компетенция		Результаты освоения ОП ВО
Код	Содержание	
1	2	3
	нормативные правовые акты в профессиональной деятельности	информационной безопасности. *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	*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

Компетенция		Результаты освоения ОП ВО
Код	Содержание	
1	2	3
	профессиональных задач	назначения.
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	*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

Компетенция		Результаты освоения ОП ВО
Код	Содержание	
1	2	3
	соответствующих проектных решений	*Владеть*: методами мониторинга и аудита, выявления 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 про-

Компетенция		Результаты освоения ОП ВО
Код	Содержание	
1	2	3
		цессов обработки, поиска и передачи информации
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 организацион-

Компетенция		Результаты освоения ОП ВО
Код	Содержание	
1	2	3
		но-распорядительных документов, регламентирующих 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,

Компетенция		Результаты освоения ОП ВО
Код	Содержание	
1	2	3
		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	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 Подготовка к сдаче и сдача государственного экзамена

Порядок проведения государственного экзамена, критерии оценки знаний студентов регламентируются Положением ПЛ 2.3.23 – 2017 «СМК Порядок проведения государственной итоговой аттестации по образовательным программам высшего образования – по программам бакалавриата, программам специалитета и программам магистратуры».

4.1. Результаты освоения ОП ВО (ГИА)

Итоговый государственный экзамен позволяет выпускнику продемонстрировать способность, опираясь на полученные знания, умения, а также используя сформированные навыки в процессе обучения, решать на современном уровне задачи своей профессиональной деятельности, профессионально излагать специальную информацию, научно аргументировать и защищать свою точку зрения.

В процессе государственного экзамена выпускник должен продемонстрировать следующие компетенции (таблица 2):

Таблица 2 – Результаты освоения ОП ВО (ГИА)

Компетенция		Результаты освоения ОП ВО
Код	Содержание	
Общекультурные компетенции		
ОК-2	способность использовать основы экономических знаний в различных сферах деятельности	*Знать*: основные понятия экономической деятельности. *Уметь*: оценивать эффективность и анализировать экономические показатели в области защиты информации. *Владеть*: навыками экономического обоснования выбранного решения.
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 профессиональной деятельности в области обеспечения информационной безопасности	*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.
ОК-7	способность к коммуникации в устной и письменной формах на	*Знать*: профессиональную терминологию на иностранном языке. *Уметь*: соблюдать речевой этикет.

Компетенция		Результаты освоения ОП ВО
Код	Содержание	
	русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности	*Владеть*: основами публичной речи.
Общепрофессиональные компетенции		
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 обосновании принципов действия средств технической защиты информации. *Владеть*: навыками анализа физических основ действия средств технической защиты информации.
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	способностью применять положения электротехники, электроники и схемотехники для решения профессиональных задач	*Знать*: принципы работы современной радиоэлектронной аппаратуры и физические процессы, протекающие в них. *Уметь*: анализировать принципы функционирования современной радиоэлектронной аппаратуры. *Владеть*: навыками обоснования принципов действия современной радиоэлектронной аппаратуры.
ОПК-5	способностью использовать нормативные правовые акты в профессиональной деятельности	*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.
Профессиональные компетенции:		

Компетенция		Результаты освоения ОП ВО
Код	Содержание	
эксплуатационная деятельность:		
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*: обосновывать меры противодействия нарушениям информационной безопасности. *Владеть*: профессиональной терминологией в области использования программных средств системного, прикладного и специального назначения.
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.
Профессиональные компетенции: проектно-технологическая деятельность:		
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*: применять модели угроз и нарушителей информационной безопасности информационных систем. *Владеть*: навыками выбора и обоснования критериев эффективности функционирования защищенных информационных систем.

Компетенция		Результаты освоения ОП ВО
Код	Содержание	
	проектных решений	
Профессиональные компетенции: экспериментально-исследовательская деятельность:		
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*: основные нормативные и методические документы в области информационной безопасности. *Уметь*: анализировать основные нормативные и методические документы в области информационной безопасности. *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.
Профессионально-специализированные компетенции направленности (профиля) N 2 «Организация и технология защиты информации (на транспорте)»:		
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-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;

Компетенция		Результаты освоения ОП ВО
Код	Содержание	
		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.

4.2. Содержание государственного экзамена

Государственный экзамен проводится в устном виде по билетам. Каждый билет содержит теоретические и практико-ориентированные вопросы. Государственный экзамен является полидисциплинарным, включает в себя материал по дисциплинам:

Дисциплина 1. Б1.Б.06 «Правовые и экономические аспекты профессиональной деятельности»

Рынок информации: особенности и проблемы развития. Понятие о рисках и их классификация. Оценка риска. Экономические проблемы информационных ресурсов. Экономическая безопасность. Информация как важнейший ресурс экономики. Риски в информационной деятельности. Оценка рисков при защите информации. Информация как товар, цена информации. Сущность себестоимости объектов интеллектуальной собственности. Основные подходы к определению затрат на защиту информации. Формирование бюджета службы защиты информации. Система ресурсообеспечения защиты информации и эффективность ее использования. Стоимостная оценка результатов противоправного использования информации. Управление ресурсами в процессе защиты информации. Информация как фактор производства и как важнейший ресурс экономики. Экономическая эффективность защиты информации.

Дисциплина 2. Б1.Б.15 «Программно-аппаратные средства защиты информации»

Классификация методов и средств защиты информации от несанкционированного доступа. Классы защищенности автоматизированных систем в соответствии с уровнями конфиденциальности. Требования к построению систем защиты информации и порядок подбора соответствующих программно-аппаратных средств. Уязвимости автоматизированной системы и выбор средств защиты информации. Управление доступом в локальную среду операционных систем. Управление доступом в сетевую среду операционных систем. Ролевое разграничение доступа к данным в современных СУБД.

Сетевые атаки. Адаптивная безопасность в вычислительных сетях. Модели взаимодействия программной закладки с атакуемой компьютерной системой. Сигнатурное и эвристическое сканирование как метод выявления программных закладок. Антивирусный мониторинг как метод выявления программных закладок. Файловые вирусы: жизненный цикл, особенности функционирования, особенности противодействия файловым вирусам. Сетевые вирусы: жизненный цикл, особенности функционирования, особенности противодействия сетевым вирусам. Скриптовые вирусы: жизненный цикл, особенности функционирования, особенности противодействия скриптовым вирусам. Стелс-технологии: назначение, методы противодействия. Способы и средства обеспечения целостности информации. Средства и методы обеспечения целостности данных СУБД. Электронная подпись. Криптографические средства обеспечения целостности информации. Модели безопасности СУБД. Средства защиты локальных операционных систем.

Дисциплина 3. Б1.Б.16 «Криптографические методы защиты информации»

Методы и алгоритмы классической симметричной криптографии. Симметричные потоковые криптографические алгоритмы. Симметричные блочные криптографические алгоритмы. Методы и алгоритмы асимметричной криптографии.

Дисциплина 4. Б1.Б.17 «Организационное и правовое обеспечение информационной безопасности»

Государственные органы Российской Федерации, контролирующие деятельность в области защиты информации: функции и полномочия ФСТЭК России; функции и полномочия ФСБ России; функции и полномочия Межведомственной комиссии по защите государственной тайны. Законодательство РФ в области защиты государственной тайны: перечень сведений, составляющих государственную тайну; отнесение сведений к государственной тайне и их засекречивание; рассекречивание сведений и их носителей; контроль и надзор за обеспечением защиты государственной тайны. Законодательство РФ в области защиты информации конфиденциального характера. Правовая защита информации конфиденциального характера: правовая защита служебной тайны; правовая защита профессиональной тайны; правовая защита коммерческой тайны; правовая защита персональных данных. Лицензирование и сертификация в области защиты информации. Служба безопасности предприятия. Резервирование оборудования и дублирование информации. Аттестация объектов информатизации. Контроль доступа в помещения: системы контроля доступа; средства поиска и досмотра.

Дисциплина 5. Б1.Б.18 «Техническая защита информации»

Каналы и системы обработки и передачи информации. Визуально-оптические каналы утечки информации. Акустические каналы утечки информации. Электромагнитные каналы утечки информации. Мероприятия по защите информации от утечки по визуально-

оптическому каналу. Мероприятия по защите информации от утечки по акустическому каналу. Мероприятия по защите информации от утечки по электромагнитному каналу: защита от утечки за счет микрофонного эффекта; защита от утечки за счет электромагнитного излучения; защита от утечки за счет паразитной генерации; защита от утечки по цепям питания; защита от утечки по цепям заземления; защита от утечки за счет взаимного влияния проводов и линий связи; защита от утечки за счет высокочастотного навязывания; защита от утечки в волоконно-оптических линиях и системах связи. Физические датчики для защиты информации: понятие о чувствительности, «мертвой зоне» и помехозащищенности физических датчиков.

Дисциплина 6. Б1.Б.25 «Физические основы защиты информации»

Расчет скорости распространения и длины волны упругих (акустических) волн в различных средах. Расчет коэффициента затухания и плотности потока мощности волн, распространяющихся в среде с акустическими потерями. Расчет коэффициента отражения и прохождения акустических волн на границе раздела сред. Расчет ориентации лучей акустических волн. Преобразование продольных и сдвиговых волн. Расчет скорости распространения и длины волны плоской электромагнитной волны, распространяющейся в среде с потерями и без потерь.

Дисциплина 7. Б1.В.03 «Управление информационной безопасностью на объектах транспортной инфраструктуры»

Основные определения системы, характеристики и свойства. Понятие системы управления информационной безопасностью. Типовая структура СУИБ. Функции СУИБ. Стандартизация в области обеспечения информационной безопасности. Международные организации по стандартизации. Обзор международных стандартов в области информационной безопасности. Стандарт ГОСТ Р ИСО/МЭК 27001 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования». Область применения, назначение, основные термины. Стандарт ГОСТ Р ИСО/МЭК 27001 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования». Обзор требований стандарта. Стандарт ГОСТ Р ИСО/МЭК 27005. «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности». Область применения, назначение, основные термины. Стандарт ГОСТ Р ИСО/МЭК 27005. «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности». Обзор требований стандарта. Стандарт ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности». Назначение стандарта. Понятия безопасности и их взаимосвязь. Процесс разработки объекта оценки. Процесс оценки

объекта оценки. Стандарт ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности». Последовательность формирования требований и спецификаций. Представление требований к безопасности. Структура требований к безопасности и требований доверия. Оценочные уровни доверия.

4.3. Перечень вопросов, выносимых на государственный экзамен

Дисциплина 1. Б1.Б.06 «Правовые и экономические аспекты профессиональной деятельности»

1. Рынок информации: особенности и проблемы развития.
2. Экономические проблемы информационных ресурсов.
3. Информация как важнейший ресурс экономики.
4. Риски в информационной деятельности. Оценка рисков при защите информации.
5. Информация как товар, цена информации.
6. Основные подходы к определению затрат на защиту информации.
7. Формирование бюджета службы защиты информации.
8. Система ресурсообеспечения защиты информации и эффективность ее использования.
9. Стоимостная оценка результатов противоправного использования информации.
10. Управление ресурсами в процессе защиты информации.
11. Информация как фактор производства и как важнейший ресурс экономики.
12. Экономическая эффективность защиты информации.

Дисциплина 2. Б1.Б.15 «Программно-аппаратные средства защиты информации»

1. Классификация методов и средств защиты информации от несанкционированного доступа.
2. Классы защищенности автоматизированных систем в соответствии с уровнями конфиденциальности.
3. Требования к построению систем защиты информации и порядок подбора соответствующих программно-аппаратных средств.
4. Уязвимости автоматизированной системы и выбор средств защиты информации.
5. Управление доступом в локальную среду операционных систем.
6. Управление доступом в сетевую среду операционных систем.
7. Ролевое разграничение доступа к данным в современных СУБД.
8. Сетевые атаки.
9. Адаптивная безопасность в вычислительных сетях.
10. Модели взаимодействия программной закладки с атакуемой компьютерной системой.

11. Сигнатурное и эвристическое сканирование как метод выявления программных закладок.
12. Антивирусный мониторинг как метод выявления программных закладок.
13. Файловые вирусы: жизненный цикл, особенности функционирования, особенности противодействия файловым вирусам.
14. Сетевые вирусы: жизненный цикл, особенности функционирования, особенности противодействия сетевым вирусам.
15. Скриптовые вирусы: жизненный цикл, особенности функционирования, особенности противодействия скриптовым вирусам.
16. Стелс-технологии: назначение, методы противодействия.
17. Способы и средства обеспечения целостности информации.
18. Средства и методы обеспечения целостности данных СУБД.
19. Электронная подпись.
20. Криптографические средства обеспечения целостности информации.
21. Модели безопасности СУБД.
22. Средства защиты локальных операционных систем.

Дисциплина 3. Б1.Б.16 «Криптографические методы защиты информации»

1. Методы и алгоритмы классической симметричной криптографии.
2. Симметричные потоковые криптографические алгоритмы.
3. Симметричные блочные криптографические алгоритмы.
4. Методы и алгоритмы асимметричной криптографии.

Дисциплина 4. Б1.Б.17 «Организационное и правовое обеспечение информационной безопасности»

1. Государственные органы Российской Федерации, контролирующие деятельность в области защиты информации.
2. Функции и полномочия ФСТЭК России
3. Функции и полномочия ФСБ России.
4. Функции и полномочия Межведомственной комиссии по защите государственной тайны.
5. Законодательство Российской Федерации в области защиты государственной тайны.
6. Перечень сведений, составляющих государственную тайну
7. Отнесение сведений к государственной тайне и их засекречивание.
8. Рассекречивание сведений и их носителей.
9. Контроль и надзор за обеспечением защиты государственной тайны.

10. Законодательство РФ в области защиты информации конфиденциального характера.
11. Правовая защита служебной тайны.
12. Правовая защита профессиональной тайны.
13. Правовая защита коммерческой тайны.
14. Правовая защита персональных данных.
15. Лицензирование и сертификация в области защиты информации.
16. Служба безопасности предприятия.
17. Резервирование оборудования и дублирование информации.
18. Аттестация объектов информатизации.
19. Контроль доступа в помещения.

Дисциплина 5. Б1.Б.18 «Техническая защита информации»

1. Каналы и системы обработки и передачи информации.
2. Визуально-оптические каналы утечки информации.
3. Акустические каналы утечки информации.
4. Электромагнитные каналы утечки информации.
5. Мероприятия по защите информации от утечки по визуально-оптическому каналу.
6. Мероприятия по защите информации от утечки по акустическому каналу.
7. Защита от утечки за счет микрофонного эффекта.
8. Защита от утечки за счет электромагнитного излучения.
9. Защита от утечки за счет паразитной генерации.
10. Защита от утечки по цепям питания.
11. Защита от утечки по цепям заземления.
12. Защита от утечки за счет взаимного влияния проводов и линий связи.
13. Защита от утечки за счет высокочастотного навязывания.
14. Защита от утечки в волоконно-оптических линиях и системах связи.
15. Физические датчики для защиты информации: понятие о чувствительности, «мертвой зоне» и помехозащищенности физических датчиков.

Дисциплина 6. Б1.Б.25 «Физические основы защиты информации»

1. Расчет скорости распространения и длины волны упругих (акустических) волн в различных средах.
2. Расчет коэффициента затухания и плотности потока мощности волн, распространяющихся в среде с акустическими потерями.
3. Расчет коэффициента отражения и прохождения акустических волн на границе раздела сред.
4. Расчет ориентации лучей акустических волн.

5. Преобразование продольных и сдвиговых волн.
6. Расчет скорости распространения и длины волны плоской электромагнитной волны, распространяющейся в среде с потерями и без потерь.

Дисциплина 7. Б1.В.03 «Управление информационной безопасностью на объектах транспортной инфраструктуры»

1. Понятие системы управления информационной безопасностью.
2. Типовая структура СУИБ. Функции СУИБ.
3. Стандартизация в области обеспечения информационной безопасности. Международные организации по стандартизации.
4. Обзор международных стандартов в области информационной безопасности.
5. Стандарт ГОСТ Р ИСО/МЭК 27001 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования». Область применения, назначение, основные термины.
6. Стандарт ГОСТ Р ИСО/МЭК 27001 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования». Обзор требований стандарта.
7. Стандарт ГОСТ Р ИСО/МЭК 27005. «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности». Область применения, назначение, основные термины.
8. Стандарт ГОСТ Р ИСО/МЭК 27005. «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности». Обзор требований стандарта.
9. Стандарт ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности». Назначение стандарта. Понятия безопасности и их взаимосвязь. Процесс разработки объекта оценки. Процесс оценки объекта оценки.
10. Стандарт ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности». Последовательность формирования требований и спецификаций. Представление требований к безопасности. Структура требований к безопасности и требований доверия. Оценочные уровни доверия.

4.4. Перечень рекомендуемой литературы для подготовки к государственному экзамену

4.4.1 Основная литература

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
1	Селина О. В.	Экономика защиты информации: методические указания к практическим занятиям по дисциплине "Экономика защиты информации" для студентов направления подготовки 10.03.01 - "Информационная безопасность" всех форм обучения	Екатеринбург: УрГУПС, 2016	http://biblioserver.usurt.ru/cgi-bin/irbis64r_13/cgiirbis_64.exe?C21COM=F&I21DBN=KN&P21DBN=KN
2	Гузенкова Е. А.	Программно-аппаратные средства защиты информации: конспект лекций для студентов направления подготовки бакалавриата 10.03.01 «Информационная безопасность» очной формы обучения	Екатеринбург: УрГУПС, 2016	http://biblioserver.usurt.ru/cgi-bin/irbis64r_13/cgiirbis_64.exe?C21COM=F&I21DBN=KN&P21DBN=KN
3	Зырянова Т. Ю.	Криптографические методы защиты информации: курс лекций для студентов направления подготовки 10.03.01 «Информационная безопасность» очной формы обучения	Екатеринбург: УрГУПС, 2016	http://biblioserver.usurt.ru/cgi-bin/irbis64r_13/cgiirbis_64.exe?C21COM=F&I21DBN=KN&P21DBN=KN
4	Чукалова Л. Г., Ганженко Н.	Организационное и правовое обеспечение информационной безопасности: конспект лекций для студентов направления подготовки 10.03.01 «Информационная безопасность»	Екатеринбург: УрГУПС, 2016	http://biblioserver.usurt.ru/cgi-bin/irbis64r_13/cgiirbis_64.exe?C21COM=F&I21DBN=KN&P21DBN=KN
5	Черенев Ю. Б.	Техническая защита информации: конспект лекций для студентов направления подготовки 10.03.01 «Информационная безопасность»	Екатеринбург: УрГУПС, 2016	http://biblioserver.usurt.ru/cgi-bin/irbis64r_13/cgiirbis_64.exe?C21COM=F&I21DBN=KN&P21DBN=KN
6	Шейдаков Н. Е., Тищенко Е. Н., Серпенинов О. В.	Физические основы защиты информации: Учебное пособие	Москва: Издательский Центр РИО, 2016	http://znanium.com/go.php?id=556661
7	Симонович В. Г., Ганженко Н.	Физические основы защиты информации: конспект лекций для студентов направления подготовки 10.03.01 «Информационная безопасность»	Екатеринбург: УрГУПС, 2016	http://biblioserver.usurt.ru/cgi-bin/irbis64r_13/cgiirbis_64.exe?C21COM=F&I21DBN=KN&P21DBN=KN
8	Зырянова Т. Ю., Паршин К. А.	Управление информационной безопасностью на объектах транспортной инфраструктуры: конспект лекций для студентов направления подготовки 10.03.01 «Информационная безопасность» очной формы обучения	Екатеринбург: УрГУПС, 2016	http://biblioserver.usurt.ru/cgi-bin/irbis64r_13/cgiirbis_64.exe?C21COM=F&I21DBN=KN&P21DBN=KN
9	Зырянова Т. Ю.	Подготовка к сдаче и сдача государственного экзамена: методические рекомендации для студентов направления подготовки 10.03.01 «Информационная безопасность» очной формы обучения	Екатеринбург: УрГУПС, 2016	http://biblioserver.usurt.ru/cgi-bin/irbis64r_13/cgiirbis_64.exe?C21COM=F&I21DBN=KN&P21DBN=KN

4.4.2 Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка

1	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	http://e.lanbook.com/books/element.php?pl1_id=59240
2	Бабаш А. В.	Криптографические методы защиты информации. Том 3: Учебно-методическое пособие	Москва: Издательский Центр РИО, 2014	http://znanium.com/go.php?id=432654
3	Шаньгин В. Ф.	Информационная безопасность компьютерных систем и сетей: Учебное пособие	Москва: Издательский Дом "ФОРУМ", 2017	http://znanium.com/go.php?id=775200
4	Поздняков, С. Н.	Дискретная математика : учебник для студентов вузов, обучающихся по направлениям "Информатика и вычислительные системы", "Информационная безопасность"	Москва : Академия, 2008.	54 экземпляра
5	Гашков С. Б., Применко Э. А., Черепнев М. А.	Криптографические методы защиты информации: учебное пособие для студентов вузов, обучающихся по направлению "Прикладная математика и информатика" и "Информационные технологии"	Москва: Академия, 2010	21 экземпляр
6	Мельников В. П., Клейменов С. А., Петраков А. М., Клейменов С. А.	Информационная безопасность и защита информации: учебное пособие для студентов вузов, обучающихся по специальности 230201- "Информационные системы и технологии"	Москва: Академия, 2009	30 экземпляров
7	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 экземпляров
8	Гальцев А.Ф.	Физические основы защиты информации: Методическое пособие для студентов спец. 090103 "Организация и технология защиты информации"	Екатеринбург: УрГУПС, 2004	27 экземпляров
9	Милославская Н. Г.	«Серия «Вопросы управление информационной безопасностью»». Выпуск 3»	Москва: Горячая линия-Телеком, 2013	http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=5180

4.4.3 Интернет-ресурсы

1	http://rzd.ru - Официальный сайт ОАО «РЖД»
2	http://www.roszeldor.ru - Официальный сайт ФАЖТ
3	http://elibrary.ru - Научная электронная библиотека
4	https://bdu.fstec.ru - Банк данных угроз безопасности информации ФСТЭК России
5	https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00 - Государственный реестр сертифицированных средств защиты информации N РОСС RU.0001.01БИ00
6	http://gostexpert.ru - ГОСТ Эксперт - единая база ГОСТов Российской Федерации
7	Автоматизированная система правовой информации на железнодорожном транспорте АСПИ ЖТ (профессиональная БД)
8	http://www.bb.usurt.ru - Электронная среда поддержки учебного процесса студентов УрГУПС

4.5. Критерии оценки результатов сдачи государственного экзамена с описанием критериев оценивания компетенций, а также шкал оценивания

Критерии оценки при проведении государственного экзамена в устной форме:

1. Оценка «Отлично» выставляется, если выпускник продемонстрировал сформированность компетенций и может реализовывать их в профессиональной деятельности инженера путей сообщения; исчерпывающе, последовательно, грамотно и логически стройно излагает ответ, без ошибок; ответ не требует дополнительных вопросов; речь хорошая, владение профессиональной терминологией свободное; не испытывает затруднений с ответом при видоизменении задания. Компетенции сформированы на эталонном уровне в соответствии с результатами оценивания компетенции, представленными в таблице 2.

2. Оценка «Хорошо» выставляется, если выпускник продемонстрировал сформированность компетенций и может реализовывать их в профессиональной деятельности инженера путей сообщения без существенных ошибок; профессиональной терминологией владеет на достаточном уровне; грамотно, логично и по существу излагает ответ, не допускает существенных ошибок и неточностей в ответе на вопросы, но изложение недостаточно систематизировано и последовательно. Формирование компетенций достигает продвинутого уровня в соответствии с результатами оценивания компетенции, представленными в таблице 2.

3. Оценка «Удовлетворительно» выставляется, если выпускник усвоил только основной программный материал, но не знает отдельных особенностей, деталей, допускает неточности, нарушает последовательность в изложении программного материала, материал не систематизирован, недостаточно правильно сформулирован, речь в основном грамотная, но бедная; владеет минимально достаточном уровнем компетенций. Освоен пороговый уровень формирования компетенций в соответствии с результатами оценивания компетенции, представленными в таблице 2.

4. Оценка «Неудовлетворительно» выставляется, если выпускник не знает значительной части программного материала, допускает существенные грубые ошибки; основное содержание материала не раскрыто; владение профессиональной терминологией слабое. Оценка неудовлетворительно выставляется, если студент отказался отвечать. Сформированный уровень компетенций недостаточен для получения положительной оценки по результатам оценивания компетенции, представленных в таблице 2.

Описание критериев оценивания компетенций, демонстрируемых на государственном экзамене, а также шкалы оценивания сформированности компетенций (таблица 3).

Таблица 3 – Критерии оценивания компетенций, проверяемых на государственном экзамене

Коды оцениваемых компетенции	Критерии оценивания	Шкала оценивания (в баллах)/ уровни сформированности компетенции
ОК-1, ОК-4, ОК-5, ОК-7, ОПК-1, ОПК-2, ОПК-3, ОПК-5, ПК-1, ПК-2, ПК-4, ПК-7, ПК-9, ПК-10, ПСК-1, ПСК-4	Демонстрируется сформированность компетенций и возможность реализовывать их в профессиональной деятельности инженера путей сообщения; исчерпывающе, последовательно, грамотно и логически стройно излагается ответ, без ошибок; ответ не требует дополнительных вопросов; речь хорошая, владение профессиональной терминологией свободное; не замечены затруднения с ответом при видоизменении задания.	5 (отлично) /3 уровень (эталонный)
	Демонстрируется сформированность компетенций и возможность реализовывать их в профессиональной деятельности инженера путей сообщения без существенных ошибок; владение профессиональной терминологией на достаточном уровне; грамотно, логично и по существу излагается ответ, не допускается существенных ошибок и неточностей в ответе на вопросы, но изложение недостаточно систематизировано и последовательно.	4 (хорошо) / 2 уровень (продвинутый)
	Замечено понимание только основного программного материла, без понимания отдельных особенностей, деталей, допускаются неточности, нарушается последовательность в изложении программного материала, материал не систематизирован, недостаточно правильно сформулирован, речь в основном грамотная, но бедная; владение минимально достаточном уровнем компетенций.	3 (удовл.) /1 уровень (пороговый)
	Не знание значительной части программного материала, допускаются существенные грубые ошибки; основное содержание материала не раскрыто; владение профессиональной терминологией слабое. Оценка неудовлетворительно выставляется, если студент	2 (неудовл.)

	отказался отвечать, хотя бы на один из вопросов билета.	

Шкала оценивания.

Решение об оценке знаний студента принимается государственной экзаменационной комиссией открытым голосованием простым большинством членов комиссии, участвующих в заседании, в случае равного количества голосов решение принимает председатель ГЭК.

Если члены ГЭК считают, что хотя бы одна из компетенций, закрепленных за государственным экзаменом в ГИА, сформирована ниже порогового уровня, результат государственного экзамена в целом оценивается на «неудовлетворительно».

Если среднее арифметическое уровней освоения компетенций, закрепленных за государственным экзаменом в ГИА, соответствует пороговому уровню, результат государственного экзамена в целом оценивается на «удовлетворительно».

Если среднее арифметическое уровней освоения компетенций, закрепленных за государственным экзаменом в ГИА, соответствует продвинутому уровню, результат государственного экзамена в целом оценивается на «хорошо».

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

4.6. Методические материалы, определяющие процедуры оценивания результатов освоения образовательной программы на государственном экзамене

Итоговая оценка по результатам государственного экзамена складывается из оценок:

- за ответы на вопросы экзаменационного билета;
- ответов на вопросы членов ГЭК.

Компоненты, подлежащие оцениванию	Оцениваемые компетенции	Лица, оценивающие сформированность компетенций
Ответы на вопросы экзаменационного билета	ОК-2, ОК-4, ОК-5, ОК-7, ОПК-1, ОПК-2, ОПК-3, ОПК-5, ПК-1, ПК-2, ПК-4, ПК-7, ПК-9, ПК-10, ПСК-1, ПСК-4	Члены ГЭК
Ответы на вопросы членов ГЭК	ОК-2, ОК-4, ОК-5, ОК-7, ОПК-1, ОПК-2, ОПК-3, ОПК-5, ПК-1, ПК-2, ПК-4, ПК-7, ПК-9, ПК-10, ПСК-1, ПСК-4	Члены ГЭК

Результаты оценивания компетенций в порядке государственного экзамена приведены в таблице 2. Шкала и критерии оценивания компетенций представлены в таблице 3.

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

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

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

4.7. Рекомендации обучающимся по подготовке к государственному экзамену

Полидисциплинарный государственный экзамен это один из завершающих этапов подготовки бакалавра, механизм выявления и оценки результатов формирования компетенций и установления соответствия уровня подготовки выпускников требованиям ФГОС ВО по направлению подготовки 10.03.01 «Информационная безопасность» направленность (профиль) «Организация и технология защиты информации (на транспорте)».

В период подготовки к государственному экзамену обучающиеся актуализируют пройденный материал, обращаются к учебным, учебно-методическим источникам, закрепляют полученные знания. Подготовка студента к государственному экзамену включает в себя два этапа: самостоятельная работа в течение всего периода обучения; непосредственная подготовка в дни, предшествующие государственному экзамену по темам разделам и темам учебных дисциплин, выносимым на государственную аттестацию.

При подготовке к государственному экзамену студентам целесообразно использовать материалы лекций, основную и дополнительную литературу и материалы интернет ресурсов (п.4.4 настоящей программы ГИА).

Государственный экзамен проводится в устном виде по билетам, формулировка вопросов которых совпадает с формулировкой перечня рекомендованных для подготовки вопросов государственного экзамена (см. п.4.3 настоящей программы ГИА), доведенного до сведения студентов не позднее чем за шесть месяцев до начала государственной итоговой аттестации (в соответствии с Положением ПЛ 2.3.23-2017 «СМК Порядок проведения государственной итоговой аттестации по образовательным программам высшего образования - по программам бакалавриата, программам специалитета и программам магистратуры».

Перед полидисциплинарным государственным экзаменом для студентов проводятся предэкзаменационные консультации, по вопросам, разделам и темам, включенным в программу государственного экзамена, которые вызывают затруднение.

Обучающимся целесообразно составить план подготовки к государственному экзамену, в котором в определенной последовательности отражается изучение или повторение всех экзаменационных вопросов.

Во время государственной аттестации члены государственной экзаменационной комиссии могут задать дополнительные вопросы, к которым студент так же должен быть готов. Дополнительные вопросы задаются членами государственной комиссии в рамках билета, в развитии темы и связаны, как правило, с неполным ответом. Уточняющие вопросы задаются, чтобы либо конкретизировать мысли студента, либо чтобы студент подкрепил те или иные теоретические положения практическими примерами, либо привлек знания смежных учебных дисциплин.

5 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты

5.1 Требования к структуре, оформлению, порядку выполнения, критериям оценки, представлению к защите выпускной квалификационной работы

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» (с изменениями от 16.05.2017 г.) .

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 «СМК 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) Адаптация изменений законодательства Российской Федерации по защите персональных данных к существующим информационным системам обработки персональных данных.

2) Адаптация информационных систем персональных данных к новым изменениям в законодательстве Российской Федерации.

3) Анализ взаимосвязи угроз и уязвимостей в системах электронного документооборота.

4) Анализ возможностей использования средств защиты информации в соответствии с требованиями руководящих документов.

5) Анализ защищенности беспроводных локальных сетей на предприятии. Меры повышения защищенности.

6) Анализ и минимизация информационного риска при передаче данных по сети общего пользования.

7) Анализ и разработка предложений по предоставлению доступа к информационным системам предприятия.

8) Анализ информационной безопасности в автоматизированных системах управления на предприятии.

9) Анализ методик защиты речевой информации в защищаемом помещении от утечки по акустическому каналу.

10) Анализ операционных систем отечественного производства на соответствие требованиям по безопасности информации.

11) Анализ эффективности применения пассивных и активных средств защиты информации при блокировании виброакустического канала утечки информации на предприятии.

12) Анализ эффективности применения технических средств для оценки характеристик защищенности помещений.

13) Аудит информационной безопасности локальной вычислительной сети.

14) Аудит информационной безопасности предприятия на соответствие международным стандартам.

15) Внедрение DLP-системы как инструмента обеспечения информационной безопасности компании.

16) Внедрение системы защищенного электронного документооборота на предприятии.

17) Внедрение системы межсетевого экранирования как инструмента обеспечения информационной безопасности коммерческого предприятия.

18) Внедрение системы обнаружения вторжений в сети предприятия, обрабатывающего персональные данные.

19) Задачи повышения защищенности электронного документооборота.

20) Защищенность беспроводных сетей на предприятии.

21) Исследование встроенных механизмов защиты информации в операционных системах и соответствие их руководящим документам по безопасности.

22) Исследование методов повышения стойкости стеганографических систем.

23) Исследование мировых тенденций в сфере обеспечения информационной безопасности.

24) Методика оценки актуальности угроз информационной безопасности в государственных информационных системах.

25) Методика построения модели нарушителя для предприятий различных форм собственности.

26) Методы обнаружения вторжений и их применение в информационных системах, обрабатывающих информацию конфиденциального характера.

27) Модернизация комплексной системы безопасности на предприятии с использованием средств криптографической защиты информации.

28) Модернизация системы контроля и управления доступом на типовом объекте транспортной инфраструктуры.

29) 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.

30) Подготовка и проведение аттестационных испытаний объекта информатизации по требованиям безопасности информации.

31) Применение облачных технологий в обеспечении информационной безопасности предприятия.

32) Проектирование защищенной системы дистанционного обучения.

33) Проектирование защищенных каналов связи корпоративной информационной системы с использованием VPN-технологий.

34) Проектирование и анализ распределенной системы видеонаблюдения на предприятии.

35) Проектирование комплексной системы защиты информации на предприятии.

36) Проектирование системы резервного копирования для информационной системы высокой доступности.

37) Разработка безопасного принципа проведения транзакций в системах электронной коммерции.

38) Разработка документации по использованию систем обнаружения вторжений в комплексных системах защиты информации.

39) Разработка и внедрение методов управления риском утечки информации из корпоративной сети предприятия.

40) Разработка и внедрение системы защиты периметра сети на предприятии.

41) Разработка и внедрение системы разграничения прав доступа в организации.

42) Разработка комплекса мероприятий по организации защиты информации в коммерческой организации.

43) Разработка мер по технической защите конфиденциальной информации в организации.

44) Разработка мер противодействия угрозам безопасности корпоративной информации со стороны сотрудников предприятия.

45) Разработка методики выявления скрытых каналов передачи информации посредством побочных электромагнитных излучений.

46) Разработка методики противодействия современным атакам на информационные системы организации.

47) Разработка методов обеспечения безопасности мобильной связи при эксплуатации на предприятии.

48) Разработка методов противодействия лазерно-акустическим средствам разведки.

49) Разработка организационных и технических мер защиты информации в автоматизированной системе управления производственными и технологическими процессами на критически важном объекте.

50) Разработка политики безопасности персональных данных при их обработке в базах данных организации.

51) Разработка политики управления инцидентами информационной безопасности на предприятии.

52) Разработка практического руководства по обеспечению информационной безопасности на предприятии.

53) Разработка рекомендаций по внедрению центра управления безопасностью в коммерческой организации.

54) Разработка системы защиты информации при проведении видеоконференций.

55) Разработка системы защиты периметра сети на предприятии.

56) Разработка системы защиты персональных данных в организации.

57) Разработка системы контроля доступа на промышленном предприятии.

58) Разработка требований для подготовки предприятия к лицензированию его длительности по технической защите конфиденциальной информации.

59) Реализация действий при срабатывании правил обработки событий на системе обнаружения атак.

60) Сравнительный анализ защищенности локальной вычислительной сети, основанной на операционных системах Windows и Linux.

5.4 Показатели и критерии оценивания компетенций, шкала оценивания

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

- 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.

Результаты защиты ВКР определяются оценками "отлично", "хорошо", "удовлетворительно", "неудовлетворительно", в соответствии с критериями оценивания. 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 бакалавра. 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 и внешняя рецензия – положительные, с оценкой не ниже «хорошо». Компетенции сформированы на эталонном уровне в соответствии с результатами оценивания компетенции, представленными в таблице 5.

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 и внешняя рецензия – положительные, с оценкой не ниже «хорошо». Формирование компетенций достигает продвинутого уровня в соответствии с результатами оценивания компетенции, представленными в таблице 5.

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 и внешняя рецензия – положительные, с оценкой не ниже «удовлетворительно». Освоен пороговый уровень формирования компетенций в соответствии с результатами оценивания компетенции, представленными в таблице 5.

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 и во внешней рецензии имеются существенные замечания. Сформированный уровень компетенций недостаточен для получения положительной оценки по результатам оценивания компетенции, представленных в таблице 5.

По завершении защиты ВКР экзаменационная комиссия на закрытом заседании обсуждает степень соответствия работы обязательным нормативным документам и существующим требованиям, уровень доклада и характер ответов каждого защищающегося, анализирует поставленные каждым членом комиссии оценки и определяет каждому студенту итоговую оценку по защите ВКР. Принцип определения итоговой оценки по защите ВКР

аналогичен определению итоговой оценки за государственный экзамен. Результаты защиты ВКР доводятся до студента сразу после закрытого заседания государственной экзаменационной комиссии.

Описание показателей и критериев оценивания компетенций, демонстрируемых с помощью ВКР, а также шкалы оценивания сформированности компетенций (таблица 4).

Таблица 4 – Критерии оценивания компетенций (защита ВКР)

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	3 (удовл.) /1 уровень (пороговый)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		информация недостаточно систематизирована и не структурирована. Логика в изложении содержания ВКР присутствует фрагментарно. 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	4 (хорошо) / 2 уровень (продвинутый)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		обоснованы.	
		В экономическом разделе ВКР четко поставлена задача оценки экономической эффективности предложенных решений. Экономический анализ содержит незначительные ошибки. Полученные выводы частично обоснованы.	3 (удовл.) /1 уровень (пороговый)
		В экономическом разделе ВКР не поставлена задача оценки экономической эффективности предложенных решений. Экономический анализ содержит значительные ошибки. Полученные выводы необоснованны.	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	2 (неудовл.)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		историческая справка по формированию и развитию рассматриваемой проблемы. Список использованных источников не содержит ссылок на литературу по истории проблемы.	
ОК-4	способен использовать основы правовых знаний в различных сферах деятельности	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.	5 (отлично) /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	2 (неудовл.)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		методических документах ФСБ России, ФСТЭК России.	
ОК-5	способен понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	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 приводит перечень соответствующих нормативных правовых актов в области информационной	3 (удовл.) /1 уровень (пороговый)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		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.)
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	3 (удовл.) /1 уровень (пороговый)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		руководителя ВКР и консультантов по разделам. Допускал нарушения календарного плана. При общении с руководителем и консультантами соблюдал профессиональную этику.	
		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.)
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	4 (хорошо) / 2 уровень (продвинутый)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		ВКР правильно используются и трактуются. При ответе на вопросы комиссии возникают затруднения в формулировке своей мысли.	
		В аннотации к ВКР а иностранном языке допущены 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.	3 (удовл.) /1 уровень (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	5 (отлично) /3 уровень (эталонный)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		тексте ВКР соответствует содержанию. Знания и умения, полученные из использованных источников, отражены в тексте ВКР и в докладе. Приведен полный анализ использованных источников.	
		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.	2 (неудовл.)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		Знания и умения, полученные из использованных источников, не отражены в тексте ВКР и в докладе. Отсутствует анализ использованных источников.	
ОК-9	способен использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности	На защите ВКР выглядит бодрым и здоровым. 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.	5 (отлично) /3 уровень (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-4	способен понимать	При оформлении текста ВКР с	5 (отлично)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
	значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	использование текстового процессора использованы все необходимые функции по форматированию текста, таблиц, рисунков, формул. Презентационные материалы выполнены на профессиональном уровне.	/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 процессора не использованы функции по форматированию текста, таблиц, рисунков, формул. Презентационные материалы отсутствуют.	2 (неудовл.)
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-	5 (отлично) /3 уровень (эталонный)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		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 комиссии.	3 (удовл.) /1 уровень (пороговый)
		Не ориентируется в нормативных правовых актах в области информационной безопасности и защиты информации, нормативных методических документах	2 (неудовл.)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		ФСБ России, ФСТЭК России. Не справляется с поставленными вопросами комиссии.	
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» отсутствует постановка задачи. Раздел выполнен не полно и с существенными ошибками. Обоснование полученных выводов отсутствует.	2 (неудовл.)
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	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	5 (отлично) /3 уровень (эталонный)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
	функционирования объекта защиты	(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 управленческого решения по реализации полученных результатов, включая организационные мероприятия по его внедрению с описанием результатов внедрения.	4 (хорошо) / 2 уровень (продвинутый)
		В ВКР приведен анализ информационной	3 (удовл.) /1 уровень

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		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.	(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.)
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	4 (хорошо) / 2 уровень (продвинутый)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		затруднениями.	
		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 задач	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, инструментальные средства, языков и систем программирования применял их с помощью руководителя и с незначительными затруднениями.	4 (хорошо) / 2 уровень (продвинутый)
		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	2 (неудовл.)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		специального назначения, инструментальные средства, языков и систем программирования не смог их применить самостоятельно.	
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 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.	4 (хорошо) / 2 уровень (продвинутый)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		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 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.	2 (неудовл.)
ПК-4	способен участвовать в работах по реализации политики информационной безопасности, применять	В ВКР приведен анализ информационной инфраструктуры объекта защиты. Приведено подробное и структурированное описание	5 (отлично) /3 уровень (эталонный)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
	комплексный подход к обеспечению информационной безопасности объекта защиты	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 управленческого решения по реализации полученных	4 (хорошо) / 2 уровень (продвинутый)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		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.)
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	5 (отлично) /3 уровень (эталонный)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		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 управленческого решения по реализации полученных результатов, включая организационные мероприятия по его	4 (хорошо) / 2 уровень (продвинутый)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		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.)
ПК-6	способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств	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.	5 (отлично) /3 уровень (эталонный)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
	защиты информации	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 управленческого решения по реализации полученных результатов, включая организационные мероприятия по его внедрению с описанием результатов внедрения.	4 (хорошо) / 2 уровень (продвинутый)
		В ВКР приведен анализ	3 (удовл.)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		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.	/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.)
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	5 (отлично) /3 уровень (эталонный)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		разработки методик анализа угроз информационной безопасности и оценки уязвимостей.	
		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 последствий. В ВКР отсутствует построение модели нарушителя и анализ уязвимостей объекта защиты.	2 (неудовл.)
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)	5 (отлично) /3 уровень (эталонный)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		апробацию результатов своей научно-исследовательской деятельности на научно-практических конференциях.	
		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 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.	3 (удовл.) /1 уровень (пороговый)
		В списке и в тексте ВКР использованных источников отсутствуют ссылки на источники научно-технической информации. Оформление текста пояснительной записки ВКР не соответствует	2 (неудовл.)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		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.	
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 и анализ.	4 (хорошо) / 2 уровень (продвинутый)
		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.)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
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 области информационной безопасности. Анализ стандартов не приводится.	3 (удовл.) /1 уровень (пороговый)
		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	Результаты экспериментов, проведенных в ходе работы над ВКР обработаны с применением	5 (отлично) /3 уровень (эталонный)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
	погрешности и достоверности их результатов	профессиональных технических и (или) программных средств.	
		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 исследований. В их описании допущены значительные ошибки.	3 (удовл.) /1 уровень (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)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		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 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	3 (удовл.) /1 уровень (пороговый)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		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.	
		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 соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	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.	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	4 (хорошо) / 2 уровень (продвинутый)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		безопасности и защиты информации, нормативные методические документы ФСБ России, ФСТЭК России.	
		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 безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности	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	5 (отлично) /3 уровень (эталонный)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		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 управленческого решения по реализации полученных результатов, включая организационные мероприятия по его внедрению с описанием результатов внедрения.	4 (хорошо) / 2 уровень (продвинутый)
		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,	3 (удовл.) /1 уровень (пороговый)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		руководящие принципы, методы, средства) для обеспечения информационной безопасности объекта защиты описаны полно, но не системно.	
		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. 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.	5 (отлично) /3 уровень (эталонный)
		Четко формулирует принципы обеспечения информационной	4 (хорошо) / 2 уровень

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		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.	(продвинутый)
		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 не в полном объеме учитывает установленные требования. В ВКР отсутствует программа и (или) методика испытаний предложенных средств и систем обеспечения информационной безопасности.	3 (удовл.) /1 уровень (пороговый)
		Не может сформулировать принципы обеспечения информационной	2 (неудовл.)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		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.	
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)
		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.	5 (отлично) /3 уровень (эталонный)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		Приводятся ссылки на современные фундаментальные научные исследования в области разработки методик анализа угроз информационной безопасности и оценки уязвимостей.	
		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 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	5 (отлично) /3 уровень (эталонный)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		решения на предприятии.	
		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 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)
		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 5), а также шкалы оценивания сформированности компетенций описаны далее по тексту.

Таблица 5 – 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 производстве	5 (отлично) /3 уровень (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)

Наименование общего показателя (критерия)	Критерии оценивания	Оценка (в баллах)/ уровень
	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)
	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	5 (отлично) /3 уровень

Наименование общего показателя (критерия)	Критерии оценивания	Оценка (в баллах)/ уровень
	соответствует требованиям	(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 общения	4 (хорошо) / 2 уровень (продвинутый)
	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)

Наименование общего показателя (критерия)	Критерии оценивания	Оценка (в баллах)/ уровень
	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 члены ГЭК считают, 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 необходимо использовать при выполнении выпускной квалификационной работы по выбранной теме:

№ п/п	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
1	Зырянова Т. Ю.	Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты:	Екатеринбург: УрГУПС, 2016	http://biblioserver.usurt.ru/cgi-bin/irbis64r_13/cgiirbis_64.exe?C21COM=F&I21DBN=KN&P21DBN=KN
2	Голицына, Попов, Максимов	Информационные системы: Учебное пособие	Москва: Издательство "ФОРУМ", 2014	http://znanium.com/go.php?id=435900
3	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	http://e.lanbook.com/books/element.php?pl1_id=59240
4	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	http://e.lanbook.com/books/element.php?pl1_id=63235
5	Партыка, Попов	Операционные системы, среды и оболочки: Учебное пособие	Москва: Издательство "ФОРУМ", 2013	http://znanium.com/go.php?id=405821
6	Кузин А. В., Кузин Д. А.	Компьютерные сети: Учебное пособие	Москва: Издательство "ФОРУМ", 2016	http://znanium.com/go.php?id=536468

7	Паршин К. А.	Оценка уровня информационной безопасности на объекте информатизации	Москва: УМЦ ЖДТ (Учебно-методический центр по образованию на железнодорожном транспорте), 2015	http://e.lanbook.com/books/element.php?pl1_id=80018
8	Милославская Н. Г.	"Серия «Вопросы управление информационной безопасностью"". Выпуск 3"	Москва: Горячая линия-Телеком, 2013	http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=5180
9	Бухтояров, Золотарев, Жуков	Поддержка принятия решений при проектировании систем защиты информации: Монография	Москва: ООО "Научно-издательский центр ИНФРА-М", 2014	http://znanium.com/go.php?id=445551
10	Кабашов	Электронное правительство. Электронный документооборот. Термины и определения: Учебное пособие	Москва: ООО "Научно-издательский центр ИНФРА-М", 2013	http://znanium.com/go.php?id=410730
11	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 экземпляров
12	Таненбаум Э.	Современные операционные системы	Санкт-Петербург: Питер, 2015	20 экземпляров
13	Партыка Т. Л., Попов И. И.	Информационная безопасность: Учебное пособие	Москва: Издательство "ФОРУМ", 2016	http://znanium.com/go.php?id=516806
14	Шейдаков Н. Е., Тищенко Е. Н., Серпенинов О. В.	Физические основы защиты информации: Учебное пособие	Москва: Издательский Центр РИО, 2016	http://znanium.com/go.php?id=556661

15	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 экземпляров
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 экземпляр
17	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 экземпляров
18	Петренко С. А., Симонов С. В.	Управление информационными рисками: экономически оправданная безопасность : информационные технологии для инженеров	Москва: ДМК Пресс, 2009	http://e.lanbook.com/books/element.php?pl1_id=40021
19	Золотарев	Управление информационной безопасностью. Ч. 1. Анализ информационных рисков	Красноярск: Сибирский государственный аэрокосмический университет имени	http://znanium.com/go.php?id=463037
20	Жукова	Управление информационной безопасностью. Ч. 2. Управление инцидентами информационной безопасности	Красноярск: Сибирский государственный аэрокосмический университет имени	http://znanium.com/go.php?id=463061
21	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 экземпляров

22	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 экземпляров
23	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	http://biblioserver.usurt.ru/cgi-bin/irbis64r_13/cgiirbis_64.exe?C21COM=F&I21DBN=KN&P21DBN=KN
24	Попова Н. П., Гущина Н. В., Шерстюченко О. А.	Безопасность жизнедеятельности: методические указания к выполнению выпускной квалификационной работы для студентов направления подготовки 10.03.01 «Информационная безопасность»	Екатеринбург: УрГУПС, 2016	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 6 – 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.	Руководитель,

Код компе-тенции	Компоненты, подлежащие оцениванию	Результаты освоения ОП ВО (ВКР)	Лица, оценивающие сформирован-ность компетенций
1	2	3	4
		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	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
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	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	проблемам с соблюдением норм профессиональной этики. *Владеть*: приемами ведения дискуссии и полемики с соблюдением норм профессиональной этики.	
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
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	Руководитель

Код компе-тенции	Компоненты, подлежащие оцениванию	Результаты освоения ОП ВО (ВКР)	Лица, оценивающие сформирован-ность компетенций
1	2	3	4
		систематизации и анализа информации.	
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-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	Руководитель, консультанты, рецензент
	Доклад на защите и презентация работы		Члены ГЭК

Код компе-тенции	Компоненты, подлежащие оцениванию	Результаты освоения ОП ВО (ВКР)	Лица, оценивающие сформирован-ность компетенций
1	2	3	4
	Ответы на вопросы членов ГЭК	охране труда и безопасности жизнедеятельности. *Владеть*: навыками безопасного использования технических средств в профессиональной деятельности.	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. *Владеть*: навыками формальной постановки и решения задачи обеспечения информационной безопасности, 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
Профессиональные компетенции, соответствующие видам профессиональной деятельности, на которые ориентирована программа бакалвриата: 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	Руководитель, рецензент
	Доклад на защите и презентация работы		Члены ГЭК
	Ответы на		Члены ГЭК

Код компе-тенции	Компоненты, подлежащие оцениванию	Результаты освоения ОП ВО (ВКР)	Лица, оценивающие сформирован-ность компетенций
1	2	3	4
	вопросы членов ГЭК	информации.	
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 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.	Руководитель, 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 обос-	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
		нования критериев эффективности функционирования защищенных информационных систем.	
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:			
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	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
		Владеть: навыками проведения физического эксперимента; методами количественного анализа процессов обработки, поиска и передачи информации	
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 членов ГЭК		Члены 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 об-	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
		ласти 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 управления 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	Руководитель, рецензент
	Доклад на защите и презентация работы		Члены ГЭК

Код компетенции	Компоненты, подлежащие оцениванию	Результаты освоения ОП ВО (ВКР)	Лица, оценивающие сформированность компетенций
1	2	3	4
	Ответы на вопросы членов ГЭК	безопасностью. *Владеть*: навыками разработки систем, комплексов, средства и технологий управления информационной безопасностью с учетом особенностей объектов защиты	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 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
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,	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
		принципы, средства) для обеспечения информационной безопасности информационных систем. *Владеть*: методами управления информационной безопасностью информационных систем.	

В качестве методических материалов, определяющих процедуру оценивания, используются положения:

ПЛ 2.3.23-2017 «СМК 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» (с изменениями от 16.05.2017 г.);

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

6 Материально-техническое и программное обеспечение государственной итоговой аттестации

Для обеспечения проведения ГИА и самостоятельной работы обучающихся на базе ФГБОУ ВО «УрГУПС» материально-техническое обеспечение включает в себя:

1) компьютерный класс - учебная аудитория для самостоятельной работы обучающихся,

– оснащение: компьютерная техника с установленным лицензионным ПО с возможностью к подключению сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета;

2) читальный зал университета,

– оснащение: специализированная мебель, компьютерная техника с возможностью к подключению сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета;

3) аудитории университета,

– оснащение: средства мультимедиа.

7 Информационные ресурсы, поисковые системы, базы данных

Таблица 7 – Информационные ресурсы

1	http://rzd.ru - Официальный сайт ОАО «РЖД»
2	http://www.roszeldor.ru - Официальный сайт ФАЖТ
3	http://elibrary.ru - Научная электронная библиотека

4	https://bdu.fstec.ru - Банк данных угроз безопасности информации ФСТЭК России
5	https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00 - Государственный реестр сертифицированных средств защиты информации N РОСС RU.0001.01БИ00
6	http://gostexpert.ru - ГОСТ Эксперт - единая база ГОСТов Российской Федерации
7	Автоматизированная система правовой информации на железнодорожном транспорте АСПИ ЖТ (профессиональная БД)
8	http://www.bb.usurt.ru - Электронная среда поддержки учебного процесса студентов УрГУПС

ПРИЛОЖЕНИЕ 1

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Уральский государственный университет путей сообщения»
(ФГБОУ ВО УрГУПС)

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Дисциплина учебного плана направления подготовки: 10.03.01
(шифр ОП)

«Информационная безопасность»
(Наименование направления подготовки)

Кафедра: Информационные технологии и защита информации
(указывается кафедра-разработчик УМК)

Б3 «Государственная итоговая аттестация»
(Шифр и наименование дисциплины в соответствии с учебным планом ОП)

Разработчик (и) УМК**:** к.т.н. Зырянова Татьяна Юрьевна

Екатеринбург
2017

Паспорт фонда оценочных средств
для государственной итоговой аттестации

Фонд оценочных средств для государственной итоговой аттестации включает в себя:

1 перечень компетенций, которыми должны овладеть обучающиеся в результате освоения образовательной программы;

2 описание показателей и критериев оценивания компетенций, а также шкал оценивания;

3 типовые контрольные задания или иные материалы, необходимые для оценки результатов освоения образовательной программы;

4 методические материалы, определяющие процедуры оценивания результатов освоения образовательной программы.

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

Компетенции обучающегося, формируемые в результате освоения образовательной программы, закреплены в матрице компетенций (Приложение 2 к ОП ВО).

Траектория формирования у обучающихся компетенций при освоении образовательной программы приведена в Программе формирования у студентов университета компетенций при освоении ОП ВО (Приложение 3.2 к ОП ВО)

2. Описание показателей и критериев оценивания компетенций, а также шкал оценивания

Показателями при оценивании компетенций являются результаты освоения ОП ВО, приведенные в программе государственной итоговой аттестации:

- Таблица 1 Результаты освоения ОП ВО;
- Таблица 2 Результаты освоения ОП ВО, которые проверяются на государственном экзамене;
- Таблица 6 Результаты освоения ОП ВО, которые проверяются на защите выпускной квалификационной работы.

Критерии, а также шкалы оценивания результатов освоения ОП ВО также закреплены в программе ГИА:

- Таблица 3 – Критерии оценивания компетенций, проверяемых на государственном экзамене;
- Таблица 4 – Критерии оценивания компетенций (защита ВКР);
- Таблица 5 – Общие критерии оценивания ВКР;
- Пункт 4.5 Показатели и критерии оценивания компетенций, шкала оценивания
- Пункт 5.4 Показатели и критерии оценивания компетенций, шкала оценивания.

3. Типовые контрольные задания или иные материалы, необходимые для оценки результатов освоения образовательной программы

3.1 Типовой экзаменационный билет

УрГУПС Кафедра ИТиЗИ 2020-2021 уч. год	ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №1 Государственный экзамен Направление подготовки бакалавров 10.03.01 «Информационная безопасность»	УТВЕРЖДАЮ: и.о. зав. каф. ИТиЗИ  Т. Ю. Зырянова

1. Правовая защита персональных данных.
2. Классификация методов и средств защиты информации от несанкционированного доступа.
3. Акустические каналы утечки информации.
4. Стандарт ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности». Назначение стандарта. Понятия безопасности и их взаимосвязь. Процесс разработки объекта оценки. Процесс оценки объекта оценки
5. Псевдослучайная последовательность задана следующим образом:

$$g_{n+2} = (g_n + g_{n+1}) mod 13,\ g_0 = 0,\ g_1 = 1.$$

а). Найдите период последовательности.

б). Является ли полученная гамма равновероятной?

Вопросы для подготовки к государственному экзамену приведены в п. 4.3 программы ГИА.

3.2 типовое задание на ВКР

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Уральский государственный университет путей сообщения»
(ФГБОУ ВО УрГУПС)

Факультет электротехнический
Кафедра «Информационные технологии и защита информации»
Направление подготовки «Информационная безопасность»

УТВЕРЖДАЮ:
и. о. заведующего кафедрой
Зырянова Татьяна Юрьевна
«17» мая 2017г.

Задание

на выпускную квалификационную работу обучающемуся
Белоносовой Надежде Николаевне
(Фамилия Имя Отчество)

1. Тема ВКР Повышение эффективности системы обеспечения информационной безопасности ЕИВЦ – структурного подразделения ГВЦ – филиала ОАО «РЖД» на основе регламентации процессов управления инцидентами информационной безопасности
утверждена приказом по университету от «17» мая 2017г. № 1083–со
2. Срок сдачи обучающимся законченного ВКР 21 июня 2017 г.
3. Исходные данные к ВКР Положение по управлению инцидентами информационной безопасности в ОАО «РЖД»;
регламент управления инцидентами ИБ в АСУ ЕСПП;
регламент процесса «Устранение инцидентов ИБ»
4. Содержание расчетно–пояснительной записки (перечень подлежащих разработке вопросов)
Характеристика объекта и предмета исследования;
совершенствование процесса «Устранение инцидентов ИБ»;
анализ затрат на совершенствование процесса «Устранение инцидентов ИБ»;
безопасность жизнедеятельности
5. Перечень демонстрационно–графического материала (с точным указанием обязательных чертежей и другого наглядного материала)
Основные стандарты и организационно–распорядительные документы ОАО «РЖД» в области управления инцидентами ИБ;
схема взаимодействия компонентов системы управления инцидентами ИБ;
основные этапы обработки инцидентов ИБ;
структура процесса «Устранение инцидентов ИБ»;
подготовка комплекса предложений по улучшению процесса «Устранение инцидентов информационной безопасности»

КАЛЕНДАРНЫЙ ПЛАН–ГРАФИК

№ п/п	Наименование этапов ВКР	Срок выполнения этапов ВКР	Примечание
1.	Изучение предметной области	17.05.17 - 21.05.17	
2.	Изучение документации	22.05.17 - 26.05.17	
3.	Выполнение теоретического раздела	27.05.17 - 01.06.17	
4.	Выполнение экономического раздела	02.06.17 - 05.06.17	
5.	Выполнение раздела "Безопасность жизнедеятельность"	06.06.17 - 08.06.17	
6.	Выполнение практического раздела	09.06.17 - 19.06.17	
7.	Оформление пояснительной записки	19.06.17 - 20.06.17	
8.	Представление на утверждение	21.06.17	
9.			
10.			

Дата выдачи задания, руководитель 17.05.17

(дата, подпись ФИО)

Задание принял к исполнению обучающийся 17.05.17

(дата, подпись ФИО)

примерный перечень тем ВКР приведен в п.5.3 программы ГИА.

3.3 Иные материалы, необходимые для оценки результатов освоения образовательной программы

При проведении процедуры ГИА также используются иные материалы, необходимые для оценки результатов освоения образовательной программы (Приведены в ПЛ 2.3.23-2017 «СМК Порядок проведения государственной итоговой аттестации по образовательным программам высшего образования - по программам бакалавриата, программам специалитета и программам магистратуры»):

- ведомость;
- протокол заседания государственной экзаменационной комиссии по проведению государственного экзамена;
- протокол заседания государственной экзаменационной комиссии по защите выпускной квалификационной работы;
- бланк оценки качества защиты для членов ГЭК;
- регламент работы ГЭК;
- памятка председателя ГЭК .

4. Методические материалы, определяющие процедуры оценивания результатов освоения образовательной программы.

Методические материалы, определяющие процедуры оценивание результатов освоения образовательной программы описаны в программе ГИА:

- п.4.6 – используемые для государственного экзамена;
- п.5.6 – используемые для защиты ВКР.

Также в качестве методических материалов, определяющих процедуру оценивания, используются положения:

ПЛ 2.3.23-2017 «СМК 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» (с изменениями от 16.05.2017 г.);

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

Лист согласования фонда оценочных материалов государственной итоговой аттестации

Направление подготовки:

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

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

Составитель, к.т.н. _____ / Т. Ю. Зырянова/
(подпись) (Ф.И.О.)

Протокол заседания кафедры № 8 от « 28 » августа 2017 г.

СОГЛАСОВАНО:

Декан Электротехнического факультета,
председатель УМК факультета _____ / В. В. Башуров /
(подпись) (Ф.И.О.)

Лист согласования к программе государственной итоговой аттестации

Направление подготовки:

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

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

Составитель, к.т.н. _____ /Т. Ю. Зырянова/
(подпись) (Ф.И.О.)

Протокол заседания кафедры № 8 от « 28 » августа 2017 г.

СОГЛАСОВАНО:

Декан Электротехнического факультета,
председатель УМК факультета _____ / В. В. Башуров /
(подпись) (Ф.И.О.)