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

«30» августа 2018 г

Утверждаю
Проректор по учебной работе
и связям с производством

_____ / Н. Ф. Сирина/

"30" августа 2018 г

ПРОГРАММА ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

Уровень высшего образования

МАГИСТРАТУРА

Направление подготовки

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

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

Квалификация
магистр

Форма обучения
очная

Екатеринбург 2018 г.

Оглавление

1 Общие положения ... 3
2 Структура государственной итоговой аттестации и ее объем ... 3
3 Перечень планируемых результатов освоения образовательной программы (ОП) ... 3
4. Подготовка к сдаче и сдача государственного экзамена ... 10
4.1. Результаты освоения ОП ВО (ГИА) ... 10
4.2. Содержание государственного экзамена ... 14
4.3. Перечень вопросов, выносимых на государственный экзамен ... 16
4.4. Перечень рекомендуемой литературы для подготовки к государственному экзамену ... 18
4.5. Критерии оценки результатов сдачи государственного экзамена с описанием критериев оценивания компетенций, а также шкал оценивания ... 21
4.6. Методические материалы, определяющие процедуры оценивания результатов освоения образовательной программы на государственном экзамене ... 23
4.7. Рекомендации обучающимся по подготовке к государственному экзамену ... 24
5. Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты ... 25
5.1. Требования к структуре, оформлению, порядку выполнения, критериям оценки, представлению к защите выпускной квалификационной работы ... 25
5.2. Процедура защиты ВКР, регламент работы государственной экзаменационной комиссии ... 25
5.3. Примерный перечень тем ВКР ... 26
5.4. Показатели и критерии оценивания компетенций, шкала оценивания ... 27
5.5. Перечень источников литературы при выполнении выпускной квалификационной работы ... 57
5.6. Методические материалы, определяющие процедуру оценивания результатов освоения образовательной программы ... 60
6. Материально-техническое и программное обеспечение государственной итоговой аттестации ... 67
7. Информационные ресурсы, поисковые системы, базы данных ... 67
ПРИЛОЖЕНИЕ 1 ... 68

1 Общие положения

Целью государственной итоговой аттестации является установление соответствия результатов освоения обучающимися образовательной программы 10.04.01 «Информационная безопасность» направленность (профиль) «Информационная безопасность 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 магистр.

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 2.3.23-2018 «СМК. Порядок проведения государственной итоговой аттестации по образовательным программам высшего образования - по программам бакалавриата, программам специалитета и программам магистратуры».

2 Структура государственной итоговой аттестации и ее объем

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) магистратуры условиям ее реализации и срокам освоения определяется ФГОС по направлению подготовки

10.04.01 «Информационная безопасность», утвержденного Приказом Министерства образования и науки Российской Федерации от 01 декабря 2016 г. № 1513.

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

проектная деятельность:

системный анализ прикладной области, выявление угроз и оценка уязвимости информационных систем, разработка требований и критериев оценки информационной безопасности; обоснование выбора состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов;

разработка систем, комплексов, средств и технологий обеспечения информационной безопасности;

разработка программ и методик, испытаний средств и систем обеспечения информационной безопасности;

научно-исследовательская деятельность:

анализ фундаментальных и прикладных проблем информационной безопасности в условиях становления современного информационного общества;

разработка планов и программ проведения научных исследований и технических разработок, подготовка отдельных заданий для исполнителей;

выполнение научных исследований с применением соответствующих физических и математических методов;

подготовка по результатам научных исследований отчетов, статей, докладов на научных конференциях;

педагогическая деятельность:

выполнение учебной (преподавательской) и методической работы в организациях, осуществляющих образовательную деятельность, по дисциплинам (модулям) соответствующих профилю подготовки;

организационно-управленческая деятельность:

организация работы коллектива исполнителей, принятие управленческих решений, определение порядка выполнения работ;

организация управления информационной безопасностью;

организация работы по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности

Российской Федерации (далее - ФСБ России), Федеральной службы по техническому и экспортному контролю Российской Федерации (далее - ФСТЭК России);

организация и выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности;

разработка проектов организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности.

Результатами освоения ОП ВО являются сформированные у выпускника знания, умения, навыки (владения) в соответствии с видами деятельности ФГОС ВО по направлению подготовки 10.04.01 «Информационная безопасность» (таблица 1).

Таблица 1 – Результаты освоения ОП ВО

Компетенция		Результаты освоения ОП ВО
Код	Содержание	
Общекультурные		
ОК-1	способность к абстрактному мышлению, анализу, синтезу	*Знать*: основные методы сбора и анализа информации, способы формализации цели и методы ее достижения. *Уметь*: анализировать, обобщать и воспринимать информацию; ставить цель и формулировать задачи по её достижению. *Владеть*: культурой мышления.
ОК-2	способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения	*Знать*: основные методологические принципы и методы исследовательской деятельности, взаимосвязь методов научного исследования; структуру и специфику научной деятельности; основы составления научных текстов и критерии научной информации. *Уметь*: выявлять проблему, на решение которой будет направлено предстоящее исследование, выбрать метод исследования, обрабатывать полученные результаты и подготовить отчет как завершающей стадии исследовательской деятельности. *Владеть*: навыками проектирования исследовательской деятельности.
Общепрофессиональные		
ОПК-1	способность к коммуникации в устной и письменной формах на государственном и одном из иностранных языков для решения задач 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

Компетенция		Результаты освоения ОП ВО
Код	Содержание	
		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.
ОПК-2	способность к самостоятельному обучению и применению новых методов исследования в профессиональной деятельности	*Знать*: алгоритм научного поиска, характеристику основных элементов научной работы. *Уметь*: осуществлять этапы поиска авторского решения. *Владеть*: навыками творческого решения задачи.
Профессиональные компетенции, соответствующие видам профессиональной деятельности, на которые ориентирована программа магистратуры: а) в проектной деятельности:		
ПК-1	способность анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты	*Знать*: направления развития информационных (телекоммуникационных) технологий; методы прогнозирования эффективности функционирования информационных систем; методы оценки затрат и рисков. *Уметь*: оценивать эффективность функционирования информационных систем. *Владеть*: навыками комплексного анализа информационных систем и автоматизированных систем на соответствие установленным требованиям.
ПК-2	способность разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности	*Знать*: этапы проектирования систем, комплексов, средства и технологий обеспечения информационной безопасности. *Уметь*: формировать требования к проектированию систем, комплексов, средства и технологий обеспечения информационной безопасности. *Владеть*: навыками разработки систем, комплексов, средства и технологий обеспечения информационной безопасности с учетом особенностей объектов защиты
ПК-3	способностью проводить обоснование состава, характеристик и	*Знать*: основные отечественные и международные стандарты информационной безопасности. *Уметь*: самостоятельно анализировать

Компетенция		Результаты освоения ОП ВО
Код	Содержание	
	функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов	отечественные и международные стандарты информационной безопасности. *Владеть*: навыками применения отечественных и международных стандартов информационной безопасности.
ПК-4	способность разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности	*Знать*: принципы обеспечения информационной безопасности объектов защиты; методики тестирования средств обеспечения информационной безопасности; современные угрозы информационной безопасности объектов. *Уметь*: анализировать угрозы информационной безопасности. *Владеть*: технологиями обеспечения информационной безопасности; средствами обеспечения информационной безопасности; средствами анализа угроз информационной безопасности.
б) в научно-исследовательской деятельности:		
ПК-5	способность анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества	*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.
ПК-6	способность осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методов и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок	*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-7	способность проводить экспериментальные исследования защищенности объектов с	*Знать*: основные понятия и методы математического анализа, теории вероятностей и математической статистики, основные понятия и методы математической логики и теории алгоритмов, дискретной ма-

Компетенция		Результаты освоения ОП ВО
Код	Содержание	
	применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента	тематики; основные понятия, законы и модели электричества и магнетизма; основные понятия, законы и модели теории колебаний и волн, оптики, акустики; особенности физических эффектов и явлений, используемых для обеспечения информационной безопасности. *Уметь*: применять основные законы физики при решении практических задач; использовать математические методы и модели для решения прикладных задач; строить математические модели задач профессиональной области *Владеть*: навыками проведения физического эксперимента; методами количественного анализа процессов обработки, поиска и передачи информации
ПК-8	способность обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи	*Знать*: принципы анализа и систематизации собранных научно-технических источников по теме исследования; основные результаты новейших исследований по проблемам информационной безопасности. *Уметь*: осуществлять поиск научной информации и работу с реферативной, справочной, периодической и монографической литературой по различным областям профессиональной деятельности; работать с научно-технической литературой по тематике профессиональной деятельности *Владеть*: навыками обработки результатов эксперимента; навыками оформления научно-технических отчетов, обзоров.
в) в педагогической деятельности:		
ПК-11	способность проводить занятия по избранным дисциплинам предметной области данного направления и разрабатывать методические материалы, используемые в образовательной деятельности	*Знать*: основные психологические характеристики личности; отражение психологических характеристик на профессиональном и личностном уровне общения. *Уметь*: использовать знания об особенностях познавательных процессов в организации трудовой деятельности; регулировать свое эмоциональное состояние и строить взаимоотношения с окружающими; ориентироваться в тенденциях развития современного педагогического процесса. *Владеть*: навыками эффективного взаимодействия с людьми; умением использовать принципы организации педагогических взаимодействий в профессиональной деятельности.
г) в организационно-управленческой деятельности:		
ПК-12	способность организовать выполнение работ, управлять коллективом исполнителей и принимать управленческие решения	*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

Компетенция		Результаты освоения ОП ВО
Код	Содержание	
		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-13	способность организовать управление информационной безопасностью	*Знать*: основные методы управления информационной безопасностью; методы аттестации уровня защищенности информационных систем; основные угрозы безопасности информации и модели нарушителя в информационных системах; принципы формирования политики информационной безопасности в информационных системах. *Уметь*: определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных систем. *Владеть*: навыками анализа информационной инфраструктуры информационной системы и ее безопасности; методами управления информационной безопасностью информационных систем.
ПК-14	способность организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России	*Знать*: основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации; правовые основы организации защиты информации конфиденциального характера; организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения технической защиты информации конфиденциального характера, по аттестации объектов информатизации и сертификации средств защиты информации. *Уметь*: применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации. *Владеть*: навыками работы с нормативными правовыми актами; методами организации и управления деятельностью служб защиты информации на предприятии; методами формирования требований по защите информации.
ПК-15	способность организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения	*Знать*: принципы организации информационных систем в соответствии с требованиями по защите информации. *Уметь*: определять информационную инфраструк-

Компетенция		Результаты освоения ОП ВО
Код	Содержание	
	информационной безопасности	туру 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.
ПК-16	способность разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности	*Знать*: основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области. *Уметь*: разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации; составлять документы на любом носителе в зависимости от назначения, содержания и вида документа. *Владеть*: навыками работы с нормативными правовыми актами; навыками работы с документами.
Дополнительные профессиональные компетенции		
ДПК-1	способность выбрать и обосновать структуру, принципы организации, комплекс средств и технологий обеспечения информационной безопасности на объектах транспортной инфраструктуры	*Знать*: правовые и организационные основы системы транспортной безопасности; состав сил и средств обеспечения транспортной безопасности. *Уметь*: оценивать критерии и необходимость применения технических средств защиты информации на объектах транспортной инфраструктуры в зависимости от характеристик объекта защиты. *Владеть*: навыками анализа нормативных правовых документов в сфере транспортной безопасности.

4. Подготовка к сдаче и сдача государственного экзамена

Порядок проведения государственного экзамена, критерии оценки знаний студентов регламентируются Положением ПЛ 2.3.23-2018 «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	
Общепрофессиональные компетенции		
ОПК-1	способность к коммуникации в устной и письменной формах на государственном и одном из иностранных языков для решения задач 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.
Профессиональные компетенции: проектная деятельность:		
ПК-1	способность анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования,	*Знать*: направления развития информационных (телекоммуникационных) технологий; методы прогнозирования эффективности функционирования информационных систем; методы оценки затрат и рисков. *Уметь*: оценивать эффективность

Компетенция		Результаты освоения ОП ВО
Код	Содержание	
	оценивать затраты и риски, формировать политику безопасности объектов защиты	функционирования информационных систем. *Владеть*: навыками комплексного анализа информационных систем и автоматизированных систем на соответствие установленным требованиям.
ПК-3	способностью проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов	*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.
Профессиональные компетенции: научно-исследовательская деятельность:		
ПК-5	способность анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества	*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.
ПК-6	способность осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методов и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок	*Знать*: методы систематизации научно-технической информации. *Уметь*: анализировать научно-техническую информацию. *Владеть*: навыков сбора, обработки, анализа и систематизации научно-технической информации.

Компетенция		Результаты освоения ОП ВО
Код	Содержание	
Профессиональные компетенции: организационно-управленческая деятельность:		
ПК-13	способность организовать управление информационной безопасностью	*Знать*: основные методы управления информационной безопасностью; основные угрозы безопасности информации и модели нарушителя в информационных системах; принципы формирования политики информационной безопасности в информационных системах. *Уметь*: определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных систем. *Владеть*: навыками анализа информационной инфраструктуры информационной системы и ее безопасности; методами управления информационной безопасностью информационных систем.
ПК-14	способность организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России	*Знать*: основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации; правовые основы организации защиты информации конфиденциального характера; организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения технической защиты информации конфиденциального характера, по аттестации объектов информатизации и сертификации средств защиты информации. *Уметь*: применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации. *Владеть*: навыками работы с нормативными правовыми актами; методами организации и управления деятельно-

Компетенция		Результаты освоения ОП ВО
Код	Содержание	
		стью служб защиты информации на предприятии; методами формирования требований по защите информации.

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.02 «Защищенные информационные системы»

Понятия «система», «информационная система», «автоматизированная система» и их взаимосвязь в рамках дисциплины. Идентификация объектов защиты. Защищаемые активы (ГОСТ Р ИСО/МЭК 15408, РД ГТК России «Руководство по разработке ПЗ и ЗБ»). ГОСТ 34.003-90 «ИТ. Комплекс стандартов на АС. АС. Термины и определения»: виды АС, виды обеспечения (математическое, лингвистическое, информационное, правовое и т.д.). Роль человека в реализации угроз. Модель нарушителя. Безопасность АС. Свойства защищенной АС («КЦД»). Способы и механизмы защиты информации. Единые критерии безопасности ИТ: целевые потребители стандарта, анализ, структура и взаимосвязь Профиля защиты и Проекта защиты. Взаимосвязь основных понятий информационной безопасности (по ГОСТ Р ИСО/МЭК 15408). Система документации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Классификация изъянов защиты по источнику, этапу появления, размещению в информационной системе. Жизненный цикл АС (ГОСТ 34.601-90). Руководящий документ «Концепция защиты СВТ и АС от НСД к информации»: понятия, принципы и средства защиты информации. Регламентация процесса создания АС (по ГОСТ 34.601-90).Содержание работ на этапах создания АС. Руководящие документы «СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации», «АС. Защита от НСД к информации. Классификация АС: требования по защите информации»: классификация СВТ, АС. Регламентация процесса создания АС (по ГОСТ 34.601-90).Содержание работ на этапах создания АС. Единые критерии: Требования безопасности: функциональные и адекватности. Таксономия требований безопасности. Техническое задание на создание защищенных АС. Структура, порядок разработки (ГОСТ 34.602-89). Сводная таблица соотношения: ОУД, классов АС, СВТ, МЭ, НДВ. Техническое задание на создание защищенных АС. Порядок оформления, согласования и утверждения (ГОСТ 34.602-89).

Дисциплина 2. Б1.Б.03 «Технологии обеспечения информационной безопасности»

Подсистема межсетевого экранирования. Подсистема обнаружения и предотвращения атак. Подсистема антивирусной защиты. Подсистема защиты от несанкционированного доступа. Подсистема анализа защищенности. Подсистема автоматизированного сбора, анализа и корреляции событий информационной безопасности. Подсистема защиты каналов связи. Подсистема защиты баз данных. Подсистема контроля целостности. Подсистема инвентаризации и контроля изменений программного обеспечения. Подсистема безопасности в беспроводных сетях. Подсистема защиты среды виртуализации. Подсистема двухфакторной аутентификации в сетевой инфраструктуре. Подсистема защиты и контроля помещений ограниченного доступа. Подсистема защищенного удаленного доступа. Подсистема защиты терминального доступа. Подсистема предотвращения утечки информации ограниченного распространения. Подсистема удостоверяющего центра. Подсистема контроля управления безопасностью конфигураций аппаратного и программного обеспечения. Подсистема контроля и управления учетными записями. Подсистема защиты и централизованного управления мобильными устройствами. Подсистема контроля действий администраторов и привилегированных пользователей. Подсистема отказоустойчивости, резервного копирования и восстановления информации.

Дисциплина 3. Б1.Б.04 «Управление информационной безопасностью»

Понятие информационного риска как основы построения СУИБ. Понятие управления информационными рисками. Цели, задачи и принципы управления информационными рисками. Понятие управления информационными рисками. Основные этапы управления информационными рисками. Формулы оценки информационного риска по двум и по трем факторам. Категории рисков. Инструментальные средства анализа информационных рисков. Обзор и сравнение. Элементы разработки СУИБ в государственных информационных системах. Элементы разработки СУИБ в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах.

Дисциплина 4. Б1.В.02 «Информационная безопасность объектов транспортной инфраструктуры»

Нормативно-правовое обеспечение вопросов транспортной безопасности. Основные принципы безопасности на объектах транспортной инфраструктуры. Основные понятия в области транспортной безопасности. Организационные основы противодействия терроризму. Государственное регулирование вопросов обеспечения транспортной безопасности. Составляющая системы транспортной безопасности, направленная на обеспечение информационной безопасности. Силы и средства обеспечения транспортной безопасности на объектах инфраструктуры железнодорожного транспорта. Способы охраны объектов транспортной инфраструктуры. Технические средства охраны.

4.3. Перечень вопросов, выносимых на государственный экзамен

Дисциплина 1. Б1.Б.02 «Защищенные информационные системы»

1. Понятия «система», «информационная система», «автоматизированная система» и их взаимосвязь в рамках дисциплины.

2. Идентификация объектов защиты. Защищаемые активы (ГОСТ Р ИСО/МЭК 15408, РД ГТК России «Руководство по разработке ПЗ и ЗБ»).

3. ГОСТ 34.003-90 «ИТ. Комплекс стандартов на АС. АС. Термины и определения»: виды АС, виды обеспечения (математическое, лингвистическое, информационное, правовое и т.д.).

4. Роль человека в реализации угроз. Модель нарушителя.

5. Безопасность АС. Свойства защищенной АС («КЦД»). Способы и механизмы защиты информации.

6. Единые критерии безопасности ИТ: целевые потребители стандарта, анализ, структура и взаимосвязь Профиля защиты и Проекта защиты.

7. Взаимосвязь основных понятий информационной безопасности (по ГОСТ Р ИСО/МЭК 15408).

8. Система документации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

9. Классификация изъянов защиты по источнику, этапу появления, размещению в информационной системе.

10. Жизненный цикл АС (ГОСТ 34.601-90).

11. Руководящий документ «Концепция защиты СВТ и АС от НСД к информации»: понятия, принципы и средства защиты информации.

12. Регламентация процесса создания АС (по ГОСТ 34.601-90).Содержание работ на этапах создания АС.

13. Руководящие документы «СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации», «АС. Защита от НСД к информации. Классификация АС: требования по защите информации»: классификация СВТ, АС.

14. Регламентация процесса создания АС (по ГОСТ 34.601-90).Содержание работ на этапах создания АС.

15. Единые критерии: Требования безопасности: функциональные и адекватности. Таксономия требований безопасности.

16. Техническое задание на создание защищенных АС. Структура, порядок разработки (ГОСТ 34.602-89).

17. Сводная таблица соотношения: ОУД, классов АС, СВТ, МЭ, НДВ.

18. Техническое задание на создание защищенных АС. Порядок оформления, согласования и утверждения (ГОСТ 34.602-89).

Дисциплина 2. Б1.Б.03 «Технологии обеспечения информационной безопасности»

1. Подсистема межсетевого экранирования.
2. Подсистема обнаружения и предотвращения атак.
3. Подсистема антивирусной защиты.
4. Подсистема защиты от несанкционированного доступа.
5. Подсистема анализа защищенности.
6. Подсистема автоматизированного сбора, анализа и корреляции событий информационной безопасности.
7. Подсистема защиты каналов связи.
8. Подсистема защиты баз данных.
9. Подсистема контроля целостности.
10. Подсистема инвентаризации и контроля изменений программного обеспечения.
11. Подсистема безопасности в беспроводных сетях.
12. Подсистема защиты среды виртуализации.
13. Подсистема двухфакторной аутентификации в сетевой инфраструктуре.
14. Подсистема защиты и контроля помещений ограниченного доступа.
15. Подсистема защищенного удаленного доступа.
16. Подсистема защиты терминального доступа.
17. Подсистема предотвращения утечки информации ограниченного распространения.
18. Подсистема удостоверяющего центра.
19. Подсистема контроля управления безопасностью конфигураций аппаратного и программного обеспечения.
20. Подсистема контроля и управления учетными записями.
21. Подсистема защиты и централизованного управления мобильными устройствами.
22. Подсистема контроля действий администраторов и привилегированных пользователей.
23. Подсистема отказоустойчивости, резервного копирования и восстановления информации.

Дисциплина 3. Б1.Б.04 «Управление информационной безопасностью»

1. Понятие информационного риска как основы построения СУИБ.
2. Понятие управления информационными рисками. Цели, задачи и принципы управления информационными рисками.
3. Понятие управления информационными рисками. Основные этапы управления информационными рисками.

4. Формулы оценки информационного риска по двум и по трем факторам. Категории рисков.

5. Инструментальные средства анализа информационных рисков. Обзор и сравнение.

6. Элементы разработки СУИБ в государственных информационных системах.

7. Элементы разработки СУИБ в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах.

Дисциплина 4. Б1.В.02 «Информационная безопасность объектов транспортной инфраструктуры»

1. Нормативно-правовое обеспечение вопросов транспортной безопасности.
2. Основные принципы безопасности на объектах транспортной инфраструктуры.
3. Основные понятия в области транспортной безопасности.
4. Организационные основы противодействия терроризму.
5. Государственное регулирование вопросов обеспечения транспортной безопасности.
6. Составляющая системы транспортной безопасности, направленная на обеспечение информационной безопасности.
7. Силы и средства обеспечения транспортной безопасности на объектах инфраструктуры железнодорожного транспорта.
8. Способы охраны объектов транспортной инфраструктуры.
9. Технические средства охраны.

4.4. Перечень рекомендуемой литературы для подготовки к государственному экзамену

4.4.1 Основная литература

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
1	Хорев П. Б.	Программно-аппаратная защита информации: Учебное пособие	Москва: Издательство «ФОРУМ», 2015	http://znanium.com/go.php?id=489084
2	Шаньгин В. Ф.	Комплексная защита информации в корпоративных системах: Учебное пособие	Москва: Издательский Дом «ФОРУМ», 2018	http://znanium.com/go.php?id=937502
3	Зырянова Т. Ю.	Защищенные информационные системы: конспект лекций для студентов направления подготовки магистратуры 10.04.01 «Информационная безопасность»	Екатеринбург: УрГУПС, 2016	http://biblioserver.usurt.ru/cgi-bin/irbis64r_13/cgiirbis_64.exe?C21COM=F&I21DBN=KN&P21DBN=KN

4	Паршин К. А.	Оценка уровня информационной безопасности на объекте информатизации: допущено Федеральным агентством железнодорожного транспорта в качестве учебного пособия для студентов вузов железнодорожного транспорта	Москва: ФГБОУ "Учеб.-метод. центр по образованию на ж.-д. трансп.", 2015	https://e.lanbook.com/book/80018
5	Зырянова Т. Ю.	Технологии обеспечения информационной безопасности объектов: конспект лекций для студентов направления подготовки 10.04.01 «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
6	Зырянова Т. Ю.	Информационная безопасность объектов транспортной инфраструктуры: конспект лекций для студентов направления подготовки магистратуры 10.04.01 «Информационная безопасность»	Екатеринбург: УрГУПС, 2016	http://biblioserver.usurt.ru/cgi-bin/irbis64r_13/cgiirbis_64.exe?C21COM=F&I21DBN=KN&P21DBN=KN
7	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
8	Зырянова Т. Ю.	Управление информационной безопасностью: конспект лекций для студентов направления подготовки магистратуры 10.04.01 «Информационная безопасность»	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 магистрантов направления подготовки 10.04.01 «Информационная безопасность»	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=59241
2	Баранова Е. К., Бабаш А. В.	Информационная безопасность и защита информации: Учебное пособие	Москва: Издательский Центр РИО, 2017	http://znanium.com/go.php?id=763644
3	Душкин А. В., Кольцов А.	Аппаратные и программные средства защиты информации: Учебное пособие	Воронеж: Издательско-полиграфический центр «Научная книга», 2016	http://znanium.com/go.php?id=923168

4	Гузенкова Е. А., Агафонов А. В., Мезенцев А. В., Синадский Н. И., Хорьков Д. А.	Технологии межсетевого экранирования и защищенной обработки информации: учебное пособие по дисциплине «Защищенные информационные системы» для студентов направления подготовки 10.04.01 – «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
5	Духан Е. И., Зырянова Т. Ю., Синадский Н. И.	Средства защиты информации: учебное пособие по дисциплине «Защищенные информационные системы» для студентов 1 курса направления подготовки 10.04.01 – «Информационная безопасность»	Екатеринбург: УрГУПС, 2016	http://biblioserver.usurt.ru/cgi-bin/irbis64r_13/cgiirbis_64.exe?C21COM=F&I21DBN=KN&P21DBN=KN
6	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
7	Бочаров Б. В.	Комплексная безопасность на железнодорожном транспорте и метрополитене. Часть 1: Транспортная безопасность на железных дорогах и метрополитене	Москва: УМЦ ЖДТ (Учебно-методический центр по образованию на железнодорожном транспорте), 2015	http://e.lanbook.com/books/element.php?pl1_id=80022
8	Зырянова Т. Ю., Захарова А. А., Ялышев Ю. И.	Управление информационными рисками: монография	Тюмень: Издательство Тюменского гос. ун-та : Виндекс, 2008	10 экземпляров
9	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
10	Золотарев	Управление информационной безопасностью. Ч. 1. Анализ информационных рисков	Красноярск: Сибирский государственный аэрокосмический университет имени академика М. Ф. Решетнева, 2010	http://znanium.com/go.php?id=463037

11	Жукова	Управление информационной безопасностью. Ч. 2. Управление инцидентами информационной безопасности	Красноярск: Сибирский государственный аэрокосмический университет имени академика М. Ф. Решетнева, 2012	http://znanium.com/go.php?id=463061

1.4.3 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
ОПК-1, ПК-1, ПК-3, ПК-5, ПК-6, ПК-13, ПК-14	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 отказался отвечать, хотя бы на один из вопросов билета.	2 (неудовл.)

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	Оцениваемые компетенции	Лица,

оцениванию		оценивающие сформированность компетенций
Ответы на вопросы экзаменационного билета	ОПК-1, ПК-1, ПК-3, ПК-5, ПК-6, ПК-13, ПК-14	Члены ГЭК
Ответы на вопросы членов ГЭК	ОПК-1, ПК-1, ПК-3, ПК-5, ПК-6, ПК-13, ПК-14	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 2.3.23-2018 «СМК. Порядок проведения государственной итоговой аттестации по образовательным программам высшего образования - по программам бакалавриата, программам специалитета и программам магистратуры»;

ПЛ 2.3.22–2018 «О формировании фонда оценочных материалов (средств)».

4.7.Рекомендации обучающимся по подготовке к государственному экзамену

Полидисциплинарный государственный экзамен - это один из завершающих этапов подготовки магистранта, механизм выявления и оценки результатов формирования компетенций и установления соответствия уровня подготовки выпускников требованиям ФГОС ВО по направлению подготовки 10.04.01 «Информационная безопасность» направленность (профиль) «Информационная безопасность 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 2.3.23-2018 «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 2.3.23-2018 «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) Автоматизация выбора средств защиты информации при выполнении требований по обеспечению безопасности персональных данных.
2) Автоматизация выбора средств защиты персональных данных на основе анализа их защищенности.
3) Адаптация средств защиты конфиденциальной информации в информационном пространстве на базе методов стеганографии.
4) Анализ и разработка правил для системы обнаружения вторжений на предприятии.
5) Внедрение и анализ подсистем PKI и электронной подписи на предприятии.
6) Защита сред облачных вычислений путём верификации программного обеспечения на наличие деструктивных свойств.
7) Исследование и адаптация методов и алгоритмов построения информационных систем в организациях.
8) Исследование и разработка методов определения наличия несанкционированного доступа в объектно-ориентированных системах.
9) Исследование криптостойкости алгоритмов поточного шифрования.
10) Исследование проблем подключения государственных и коммерческих организаций к ГосСОПКА в соответствии с требованиями Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации».
11) Исследование системы защиты информационного взаимодействия в сфере облачных вычислений.
12) Методы снижения вероятности реализации угроз безопасности информации, обусловленных человеческим фактором.
13) Обеспечение безопасности критической информационной инфраструктуры согласно требованиям Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации».
14) Обеспечение информационной безопасности при использовании облачной инфраструктуры.
15) Оптимизация методики оценки защищенности речевой информации от утечки по техническим каналам.
16) Оптимизация методики снижения рисков информационной безопасности облачных сервисов на основе квантифицирования уровней защищенности и оптимизации состава ресурсов.
17) Разработка алгоритмов тестирования псевдослучайных последовательностей и хеширования данных на основе математических моделей.

18) Разработка и исследование модели и алгоритма выявления недекларированных возможностей в автоматизированных системах.
19) Разработка метода повышения информационной безопасности открытых источников сети Интернет посредством мониторинга и аудита.
20) Разработка методики автоматизированного обнаружения конфликтов в комплексе программных средств защиты информации компьютерной системы.
21) Разработка методики выявления недекларированных возможностей программ с использованием структурированных метрик сложности.
22) Разработка методики принятия решений для повышения безопасности программного обеспечения.
23) Разработка методики оценки состояния защиты информации на объекте посредством адаптации его к мировым стандартам безопасности.
24) Разработка методов анализа защищенности баз данных на основе формализации требований целостности.
25) Разработка методологии защиты видеоинформации с различной степенью конфиденциальности.
26) Разработка методологии усиления свойств защищенности криптосхем.
27) Разработка модели оценки и обеспечения информационной безопасности автоматизированных систем управления критическими объектами.
28) Разработка модели оценки и обеспечения информационной безопасности объекта информационной инфраструктуры на предприятии ОАО «РЖД».
29) Разработка системы защиты информации от угроз нарушения целостности в высокоскоростных каналах передачи данных.

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 магистранта. 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 к абстрактному мышлению, анализу, синтезу	Четко сформулированы цель и задачи ВКР Представленная в ВКР информация систематизирована и	5 (отлично) /3 уровень (эталонный)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		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.	
		Четко сформулированы цель и задачи ВКР. Представленная в ВКР информация систематизирована и структурирована Присутствует логика в изложении содержания ВКР. В целом успешный, но содержащий отдельные пробелы анализ альтернативных вариантов решения исследовательских задач. Быстро и уверенно отвечает на поставленные вопросы комиссии.	4 (хорошо) / 2 уровень (продвинутый)
		Нечетко сформулированы цель и задачи ВКР. Представленная в ВКР информация недостаточно систематизирована и не структурирована. Логика в изложении содержания ВКР присутствует фрагментарно. В целом успешный, но не систематически осуществляемый анализ альтернативных вариантов решения исследовательских задач. Частично справляется с поставленными вопросами комиссии.	3 (удовл.) /1 уровень (пороговый)
		Не сформулированы цель и	2 (неудовл.)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		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.	
ОК-2	способен самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения	Список использованных источников достаточно объемен, систематизирован, отражает тематику всех разделов ВКР. Расстановка ссылок на использованные источники в тексте ВКР соответствует содержанию. Знания и умения, полученные из использованных источников, отражены в тексте ВКР и в докладе. Приведен полный анализ использованных источников.	5 (отлично) /3 уровень (эталонный)
		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)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		Список использованных источников систематизирован, но не отражает тематику всех разделов ВКР. Расстановка ссылок на использованные источники в тексте ВКР соответствует содержанию. Знания и умения, полученные из использованных источников, отражены в тексте ВКР и в докладе. Приведен частичный анализ использованных источников.	3 (удовл.) /1 уровень (пороговый)
		Список использованных источников составлен формально и несистематически. Ссылки на использованные источники в тексте ВКР расставлены случайным образом. Знания и умения, полученные из использованных источников, не отражены в тексте ВКР и в докладе. Отсутствует анализ использованных источников.	2 (неудовл.)
ОПК-1	способен к коммуникации в устной и письменной формах на государственном и одном из иностранных языков для решения задач профессиональной деятельности	Аннотация к ВКР на 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 на иностранном языке написана с незначительными ошибками.	4 (хорошо) / 2 уровень (продвинутый)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		Грамотно и внятно строит доклад на государственном языке. Текст ВКР написан без ошибок. Все профессиональные термины на иностранном языке, встречающиеся в тексте ВКР правильно используются и трактуются. При ответе на вопросы комиссии возникают затруднения в формулировке своей мысли.	
		Аннотация к ВКР на иностранном языке написана с существенными ошибками. 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	2 (неудовл.)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		вопросы комиссии.	
ОПК-2	способность к самостоятельному обучению и применению новых методов исследования в профессиональной деятельности	Текст ВКР структурирован. Сформулированы цель и задачи исследования. Представлено авторское решение задачи, продемонстрирован творческий подход.	5 (отлично) /3 уровень (эталонный)
		Текст ВКР структурирован. Сформулированы цель и задачи исследования. Представлено авторское решение задачи.	4 (хорошо) / 2 уровень (продвинутый)
		Текст ВКР структурирован. Сформулированы цель и задачи исследования. Частично представлено авторское решение задачи.	3 (удовл.) /1 уровень (пороговый)
		Текст ВКР не структурирован. Отсутствует постановка цели и задач исследования.	2 (неудовл.)
ПК-1	способен анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты	Правильно использует и трактует термины информационных (телекоммуникационных) технологий и информационной безопасности. В ВКР присутствует комплексный анализ эффективности предложенных проектных решений, базирующийся на методах анализа затрат и рисков, а также анализ на соответствие установленным требованиям в области информационной безопасности.	5 (отлично) /3 уровень (эталонный)
		Правильно использует и трактует термины информационных (телекоммуникационных) технологий и информационной безопасности. В ВКР присутствует анализ эффективности предложенных проектных решений, частично	4 (хорошо) / 2 уровень (продвинутый)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		базирующийся на методах анализа затрат и рисков, а также анализ на соответствие установленным требованиям в области информационной безопасности.	
		Допускает ошибки в использовании и трактовке терминов информационных (телекоммуникационных) технологий и информационной безопасности. В ВКР присутствует частичный анализ эффективности предложенных проектных решений, не базирующийся на методах анализа затрат и рисков. Анализ предложенных проектных решений на соответствие требованиям информационной безопасности фрагментарен и неполон.	3 (удовл.) /1 уровень (пороговый)
		Не знает базовых терминов и понятий информационных (телекоммуникационных) технологий и информационной безопасности. В ВКР отсутствует анализ эффективности предложенных проектных решений, анализ предложенных проектных решений на соответствие требованиям информационной безопасности.	2 (неудовл.)
ПК-2	способен разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности	Демонстрирует четкое понимание процесса проектирования систем, комплексов, средств и технологий обеспечения информационной безопасности. В ВКР полно отражены требования к проектированию систем, комплексов, средств и	5 (отлично) /3 уровень (эталонный)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		технологий обеспечения информационной безопасности, являющихся объектов исследования. Продемонстрированы навыки разработки систем, комплексов, средств и технологий обеспечения информационной безопасности с учетом особенностей объекта защиты.	
		Допускает неточности в описании процесса проектирования систем, комплексов, средств и технологий обеспечения информационной безопасности. В ВКР полно отражены требования к проектированию систем, комплексов, средств и технологий обеспечения информационной безопасности, являющихся объектов исследования. Продемонстрированы навыки разработки систем, комплексов, средств и технологий обеспечения информационной безопасности.	4 (хорошо) / 2 уровень (продвинутый)
		Имеет неполное представление об этапах проектирования систем, комплексов, средств и технологий обеспечения информационной безопасности. В ВКР частично отражены требования к проектированию систем, комплексов, средств и технологий обеспечения информационной безопасности, являющихся объектов исследования. Продемонстрированы фрагментарные навыки разработки систем,	3 (удовл.) /1 уровень (пороговый)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		комплексов, средств и технологий обеспечения информационной безопасности.	
		Не имеет представления об этапах проектирования систем, комплексов, средств и технологий обеспечения информационной безопасности. В ВКР не отражены требования к проектированию систем, комплексов, средств и технологий обеспечения информационной безопасности, являющихся объектов исследования. Не продемонстрированы навыки разработки систем, комплексов, средств и технологий обеспечения информационной безопасности.	2 (неудовл.)
ПК-3	способен проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов	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)

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

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		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.	
		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 безопасности, привести примеры методик тестирования средств	2 (неудовл.)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		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.	
ПК-5	способен анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества	Приведен полный анализ уязвимостей объекта защиты на обобщенном уровне. Построены детальные модели угроз и нарушителя используются, применительно к конкретному объекту защиты, с учетом современных проблем информационной безопасности. Приводятся ссылки на современные фундаментальные научные исследования в области разработки методик анализа угроз информационной безопасности и оценки уязвимостей.	5 (отлично) /3 уровень (эталонный)
		Приведен полный анализ уязвимостей объекта защиты на обобщенном уровне. Построены детальные модели угроз и нарушителя используются, применительно к конкретному объекту защиты, с учетом современных проблем информационной безопасности.	4 (хорошо) / 2 уровень (продвинутый)
		Приведен анализ уязвимостей	3 (удовл.)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		объекта защиты на обобщенном уровне. В качестве модели угроз и модели нарушителя используются типовые модели, не учитываются современные проблемы информационной безопасности.	/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-6	способен осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методов и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок	В списке и в тексте ВКР использованных источников имеются ссылки на источники научно-технической информации, проведен их критический анализ. В ВКР приведен подробный и соответствующий содержанию ВКР план научного исследования и ожидаемые результаты.	5 (отлично) /3 уровень (эталонный)
		В списке и в тексте ВКР использованных источников имеются ссылки на источники научно-технической информации. В ВКР приведен подробный и соответствующий содержанию ВКР план научного исследования и ожидаемые результаты.	4 (хорошо) / 2 уровень (продвинутый)
		В списке и в тексте ВКР использованных источников имеются ссылки на источники научно-технической информации. В ВКР приведен план научного исследования и ожидаемые результаты, но он не достаточно полно отражает суть дальнейшего содержания	3 (удовл.) /1 уровень (пороговый)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		ВКР.	
		В списке и в тексте ВКР использованных источников отсутствуют ссылки на источники научно-технической информации. В ВКР не приведен план научного исследования и ожидаемые результаты.	2 (неудовл.)
ПК-7	способен проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента	В ВКР обоснованно и правильно применяются математические методы исследования защищенности объектов. Демонстрирует глубокое понимание физических эффектов и явлений, используемых для обеспечения информационной безопасности с учетом особенностей объекта защиты. Применяет профессиональные технические и (или) программные средства для обработки результатов эксперимента.	5 (отлично) /3 уровень (эталонный)
		В ВКР обоснованно и правильно применяются математические методы исследования защищенности объектов. Демонстрирует понимание основных физических эффектов и явлений, используемых для обеспечения информационной безопасности. Применяет базовые технические и (или) программные средства для обработки результатов эксперимента.	4 (хорошо) / 2 уровень (продвинутый)
		В ВКР применяются математические методы исследования защищенности объектов, но при этом допускаются ошибки и неточности.	3 (удовл.) /1 уровень (пороговый)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		Демонстрирует непонимание основных физических эффектов и явлений, используемых для обеспечения информационной безопасности. Не применяет технические и (или) программные средства для обработки результатов эксперимента.	
		В ВКР не применяются или применяются с существенными ошибками математические методы исследования защищенности объектов. Демонстрирует непонимание основных физических эффектов и явлений, используемых для обеспечения информационной безопасности. Не применяет технические и (или) программные средства для обработки результатов эксперимента.	2 (неудовл.)
ПК-8	способен обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи	Результаты экспериментов, проведенных в ходе работы над ВКР обработаны с применением профессиональных технических и (или) программных средств. 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.	
		Результаты экспериментов, проведенных в ходе работы над ВКР обработаны с применением базовых технических и (или) программных средств. 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)
		Результаты экспериментов, проведенных в ходе работы над ВКР обработаны без применения технических и (или) программных средств. 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-	3 (удовл.) /1 уровень (пороговый)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		исследовательской деятельности на научно-практических конференциях.	
		Результаты экспериментов, проведенных в ходе работы над ВКР не обработаны. В списке и в тексте ВКР использованных источников отсутствуют ссылки на источники научно-технической информации. Оформление текста пояснительной записки ВКР не соответствует установленным требованиям. В списке использованных источников отсутствуют ссылки на собственные публикации в научных изданиях и (или) апробацию результатов своей научно-исследовательской деятельности на научно-практических конференциях.	2 (неудовл.)
ПК-11	способность проводить занятия по избранным дисциплинам предметной области данного направления и разрабатывать методические материалы, используемые в образовательной деятельности	В ВКР приведен раздел, содержащий разработку учебно-методических рекомендаций по тематике исследования и использование современных педагогических тенденций. Приведены сведения об участии в проведении практического занятия и (или) лабораторной работы со студентами по тематике исследования под контролем преподавателя. 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)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		В ВКР приведен раздел, содержащий разработку учебно-методических рекомендаций по тематике исследования и использование современных педагогических тенденций. 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 ВКР приведен раздел, содержащий разработку учебно-методических рекомендаций по тематике исследования. 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 ВКР не приведен раздел, содержащий разработку учебно-методических рекомендаций по тематике исследования. 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-	2 (неудовл.)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		этических норм делового общения.	
ПК-12	способность организовать выполнение работ, управлять коллективом исполнителей и принимать управленческие решения	В ВКР присутствует подробное описание управленческого решения по реализации полученных результатов, включая организационные мероприятия по его внедрению с описанием результатов внедрения. К ВКР прилагается акт внедрения предложенного решения на предприятии.	5 (отлично) /3 уровень (эталонный)
		В ВКР присутствует подробное описание управленческого решения по реализации полученных результатов, включая организационные мероприятия по его внедрению с описанием результатов внедрения.	4 (хорошо) / 2 уровень (продвинутый)
		В ВКР присутствует теоретическое обоснование управленческого решения по реализации полученных результатов, включая организационные мероприятия по его внедрению.	3 (удовл.) /1 уровень (пороговый)
		В ВКР не приведено управленческое решение по реализации полученных результатов.	2 (неудовл.)
ПК-13	способность организовать управление информационной безопасностью	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
		(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-14	способность организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России	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	5 (отлично) /3 уровень (эталонный)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		защите информации применительно к объекту исследования.	
		При формулировке управленческого решения по организации внедрения результатов исследования в числе прочего опирается на нормативные правовые акты в области информационной безопасности и защиты информации, нормативные методические документы ФСБ России, ФСТЭК России.	4 (хорошо) / 2 уровень (продвинутый)
		При формулировке требований к обеспечению информационной безопасности объекта защиты приводит перечень соответствующих нормативных правовых актов в области информационной безопасности и защиты информации, нормативных методических документа ФСБ России, ФСТЭК России, но данный перечень неполон и не систематизирован.	3 (удовл.) /1 уровень (пороговый)
		Не ориентируется в нормативных правовых актах в области информационной безопасности и защиты информации, нормативных методических документах ФСБ России, ФСТЭК России.	2 (неудовл.)
ПК-15	способность организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности	При ответе на вопросы комиссии может сформулировать принципы организации информационных систем в соответствии с требованиями по защите информации. Приведено решение по вводу в эксплуатацию систем и средств обеспечения информационной безопасности, которые могут быть разработаны на	5 (отлично) /3 уровень (эталонный)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
		основании полученных в ВКР результатов с подробным описанием применяемых организационных механизмов.	
		При ответе на вопросы комиссии может сформулировать принципы организации информационных систем в соответствии с требованиями по защите информации. Приведено решение по вводу в эксплуатацию систем и средств обеспечения информационной безопасности, которые могут быть разработаны на основании полученных в ВКР результатов.	4 (хорошо) / 2 уровень (продвинутый)
		При ответе на вопросы комиссии может сформулировать принципы организации информационных систем в соответствии с требованиями по защите информации. Отсутствуют решения по вводу в эксплуатацию полученных в ВКР результатов.	3 (удовл.) /1 уровень (пороговый)
		Не демонстрирует знания принципов организации информационных систем в соответствии с требованиями по защите информации. Отсутствуют решения по вводу в эксплуатацию полученных в ВКР результатов.	2 (неудовл.)
ПК-16	способность разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности,	В ВКР приводятся проекты организационно-распорядительных документов, имеющие подробный, структурированный и обоснованный характер, отражающий особенности объекта защиты.	5 (отлично) /3 уровень (эталонный)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
	технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности	Приводятся элементы разработанной технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности.	
		В ВКР приводятся проекты организационно-распорядительных документов, имеющие подробный, структурированный и обоснованный характер, отражающий особенности объекта защиты.	4 (хорошо) / 2 уровень (продвинутый)
		В ВКР приводятся проекты организационно-распорядительных документов, регламентирующих работу по защите информации, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности, но они имеют формальный характер, не отражающий особенностей объекта защиты.	3 (удовл.) /1 уровень (пороговый)
		В ВКР не приводятся проекты организационно-распорядительных документов, регламентирующих работу по защите информации, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности.	2 (неудовл.)
ДПК-1	способность выбрать и обосновать структуру, принципы организации, комплекс средств и	Ориентируется в нормативных правовых актах, нормативных методических документах в области обеспечения информационной	5 (отлично) /3 уровень (эталонный)

Код компетенции /общие критерии оценки ВКР	Показатели оценивания	Критерии оценивания	Оценка (в баллах)/ уровни сформированности компетенции
	технологий обеспечения информационной безопасности на объектах транспортной инфраструктуры	безопасности на объектах транспортной инфраструктуры. В ВКР присутствуют выводы о возможности применения полученных результатов на объектах транспортной инфраструктуры, а также предложены элементы возможных решений по применению полученных в ВКР результатов на объектах транспортной инфраструктуры.	
		Ориентируется в нормативных правовых актах, нормативных методических документах в области обеспечения информационной безопасности на объектах транспортной инфраструктуры. В ВКР отсутствуют выводы о возможности применения полученных результатов на объектах транспортной инфраструктуры.	4 (хорошо) / 2 уровень (продвинутый)
		Демонстрирует осведомленность об особенностях обеспечения информационной безопасности на объектах транспортной инфраструктуры.	3 (удовл.) /1 уровень (пороговый)
		Не демонстрирует осведомленности об особенностях обеспечения информационной безопасности на объектах транспортной инфраструктуры.	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:

5.5.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
1	Хорев П. Б.	Программно-аппаратная защита информации: Учебное пособие	Москва: Издательство «ФОРУМ», 2015	http://znanium.com/go.php?id=489084
2	Шаньгин В. Ф.	Комплексная защита информации в корпоративных системах: Учебное пособие	Москва: Издательский Дом «ФОРУМ», 2018	http://znanium.com/go.php?id=937502
3	Зырянова Т. Ю.	Защищенные информационные системы: конспект лекций для студентов направления подготовки магистратуры 10.04.01 «Информационная безопасность»	Екатеринбург: УрГУПС, 2016	http://biblioserver.usurt.ru/cgi-bin/irbis64r_13/cgiirbis_64.exe?C21COM=F&I21DBN=KN&P21DBN=KN
4	Паршин К. А.	Оценка уровня информационной безопасности на объекте информатизации: допущено Федеральным агентством железнодорожного транспорта в качестве учебного пособия для студентов вузов железнодорожного транспорта	Москва: ФГБОУ "Учеб.-метод. центр по образованию на ж.-д. трансп.", 2015	https://e.lanbook.com/book/80018
5	Зырянова Т. Ю.	Технологии обеспечения информационной безопасности объектов: конспект лекций для студентов направления подготовки 10.04.01 «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
6	Зырянова Т. Ю.	Информационная безопасность объектов транспортной инфраструктуры: конспект лекций для студентов направления подготовки магистратуры 10.04.01 «Информационная безопасность»	Екатеринбург: УрГУПС, 2016	http://biblioserver.usurt.ru/cgi-bin/irbis64r_13/cgiirbis_64.exe?C21COM=F&I21DBN=KN&P21DBN=KN
7	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
8	Зырянова Т. Ю.	Управление информационной безопасностью: конспект лекций для студентов направления подготовки магистратуры 10.04.01 «Информационная безопасность»	Екатеринбург: УрГУПС, 2016	http://biblioserver.usurt.ru/cgi-bin/irbis64r_13/cgiirbis_64.exe?C21COM=F&I21DBN=KN&P21DBN=KN
9	Сирина Н. Ф., Зырянова Т. Ю.	Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты: методические рекомендации для магистрантов направления подготовки 10.04.01 «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
10	Шкляр М. Ф.	Основы научных исследований: учебное пособие	Москва: Дашков и К, 2013	http://znanium.com/go.php?id=415019
11	Григорович Л.А., Марцинковская Т.Д.	Педагогика и психология: Учебное пособие для студентов вузов	Москва: Гардарики, 2006	20 экземпляров

5.5.2. 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=59241
2	Баранова Е. К., Бабаш А. В.	Информационная безопасность и защита информации: Учебное пособие	Москва: Издательский Центр РИО, 2017	http://znanium.com/go.php?id=763644
3	Душкин А. В., Кольцов А.	Аппаратные и программные средства защиты информации: Учебное пособие	Воронеж: Издательско-полиграфический центр «Научная книга», 2016	http://znanium.com/go.php?id=923168
4	Гузенкова Е. А., Агафонов А. В., Мезенцев А. В., Синадский Н. И., Хорьков Д. А.	Технологии межсетевого экранирования и защищенной обработки информации: учебное пособие по дисциплине «Защищенные информационные системы» для студентов направления подготовки 10.04.01 – «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
5	Духан Е. И., Зырянова Т. Ю., Синадский Н. И.	Средства защиты информации: учебное пособие по дисциплине «Защищенные информационные системы» для студентов 1 курса направления подготовки 10.04.01 – «Информационная безопасность»	Екатеринбург: УрГУПС, 2016	http://biblioserver.usurt.ru/cgi-bin/irbis64r_13/cgiirbis_64.exe?C21COM=F&I21DBN=KN&P21DBN=KN
6	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

7	Бочаров Б. В.	Комплексная безопасность на железнодорожном транспорте и метрополитене. Часть 1: Транспортная безопасность на железных дорогах и метрополитене	Москва: УМЦ ЖДТ (Учебно-методический центр по образованию на железнодорожном транспорте), 2015	http://e.lanbook.com/books/element.php?pl1_id=80022
8	Зырянова Т. Ю., Захарова А. А., Ялышев Ю. И.	Управление информационными рисками: монография	Тюмень: Издательство Тюменского гос. ун-та : Виндекс, 2008	10 экземпляров
9	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
10	Золотарев	Управление информационной безопасностью. Ч. 1. Анализ информационных рисков	Красноярск: Сибирский государственный аэрокосмический университет имени академика М. Ф. Решетнева, 2010	http://znanium.com/go.php?id=463037
11	Жукова	Управление информационной безопасностью. Ч. 2. Управление инцидентами информационной безопасности	Красноярск: Сибирский государственный аэрокосмический университет имени академика М. Ф. Решетнева, 2012	http://znanium.com/go.php?id=463061

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;
- текста ВКР – оценивают руководитель, рецензент;
- 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*: основные методы сбора и анализа информации, способы формализации цели и методы ее достижения.	Научный руководитель, рецензент
	Ответы на вопросы членов ГЭК	*Уметь*: анализировать, обобщать и воспринимать информацию; ставить цель и формулировать задачи по её достижению. *Владеть*: культурой мышления.	Члены ГЭК
ОК-2	Текст ВКР	*Знать*: основные методологические принципы и методы исследовательской деятельности, взаимосвязь методов научного исследования; структуру и специфику научной деятельности; основы составления научных текстов и критерии научной информации. *Уметь*: выявлять проблему, на решение которой будет направлено предстоящее исследование, выбрать метод исследования, обрабатывать полученные результаты и подготовить отчет как завершающей стадии исследовательской деятельности. *Владеть*: навыками проектирования исследовательской деятельности.	Научный руководитель, рецензент
	Доклад на защите и презентация работы		Члены ГЭК
Общепрофессиональные			
ОПК-1	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	Научный 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
		процессе делового общения на иностранном языке.	
ОПК-2	Текст ВКР	*Знать*: алгоритм научного поиска, характеристику основных элементов научной работы. *Уметь*: осуществлять этапы поиска авторского решения. *Владеть*: навыками творческого решения задачи.	Научный руководитель, рецензент
Профессиональные компетенции, соответствующие видам профессиональной деятельности, на которые ориентирована программа магистратуры: а) в проектной деятельности:			
ПК-1	Текст ВКР	*Знать*: направления развития информационных (телекоммуникационных) технологий; методы прогнозирования эффективности функционирования информационных систем; методы оценки затрат и рисков. *Уметь*: оценивать эффективность функционирования информационных систем. *Владеть*: навыками комплексного анализа информационных систем и автоматизированных систем на соответствие установленным требованиям.	Научный руководитель, рецензент
	Доклад на защите и презентация работы		Члены ГЭК
	Ответы на вопросы членов ГЭК		Члены ГЭК
ПК-2	Текст ВКР	*Знать*: этапы проектирования систем, комплексов, средства и технологий обеспечения информационной безопасности. *Уметь*: формировать требования к проектированию систем, комплексов, средства и технологий обеспечения информационной безопасности. *Владеть*: навыками разработки систем, комплексов, средства и технологий обеспечения информационной безопасности с учетом особенностей объектов защиты	Научный руководитель, рецензент
	Доклад на защите и презентация работы		Члены ГЭК
	Ответы на вопросы членов ГЭК		Члены ГЭК
ПК-3	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.	Научный руководитель, рецензент
	Доклад на защите и презентация работы		Члены ГЭК
	Ответы на вопросы членов ГЭК		Члены ГЭК
ПК-4	Текст ВКР	*Знать*: принципы обеспечения информационной безопасности объектов защиты; методики тестирования средств обеспечения	Научный руководитель, рецензент

Код компетенции	Компоненты, подлежащие оцениванию	Результаты освоения ОП ВО (ВКР)	Лица, оценивающие сформированность компетенций
1	2	3	4
	Доклад на защите и презентация работы	информационной безопасности; современные угрозы информационной безопасности объектов. *Уметь*: анализировать угрозы информационной безопасности. *Владеть*: технологиями обеспечения информационной безопасности; средствами обеспечения информационной безопасности; средствами анализа угроз информационной безопасности.	Члены ГЭК
	Ответы на вопросы членов ГЭК		Члены ГЭК
б) в научно-исследовательской деятельности:			
ПК-5	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.	Научный руководитель, рецензент
	Доклад на защите и презентация работы		Члены ГЭК
	Ответы на вопросы членов ГЭК		Члены ГЭК
ПК-6	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.	Научный руководитель, рецензент
ПК-7	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.	Научный 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
		Уметь: применять основные законы физики при решении практических задач; использовать математические методы и модели для решения прикладных задач; строить математические модели задач профессиональной области *Владеть*: навыками проведения физического эксперимента; методами количественного анализа процессов обработки, поиска и передачи информации	
ПК-8	Текст ВКР	*Знать*: принципы анализа и систематизации собранных научно-технических источников по теме исследования; основные результаты новейших исследований по проблемам информационной безопасности. *Уметь*: осуществлять поиск научной информации и работу с реферативной, справочной, периодической и монографической литературой по различным областям профессиональной деятельности; работать с научно-технической литературой по тематике профессиональной деятельности *Владеть*: навыками обработки результатов эксперимента; навыками оформления научно-технических отчетов, обзоров.	Научный руководитель, рецензент
в) в педагогической деятельности:			
ПК-11	Текст ВКР	*Знать*: основные психологические характеристики личности; отражение психологических характеристик на профессиональном и личностном уровне общения. *Уметь*: использовать знания об особенностях познавательных процессов в организации трудовой деятельности; регулировать свое эмоциональное состояние и строить взаимоотношения с окружающими; ориентироваться в тенденциях развития современного педагогического процесса. *Владеть*: навыками эффективного взаимодействия с людьми; умением использовать принципы организации педагогических взаимодействий в профессиональной деятельности.	Научный руководитель, рецензент
	Доклад на защите и презентация работы		Члены ГЭК
	Ответы на вопросы членов ГЭК		Члены ГЭК
г) в организационно-управленческой деятельности:			
ПК-12	Текст 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 руково-	Научный руководитель, рецензент

Код компетенции	Компоненты, подлежащие оцениванию	Результаты освоения ОП ВО (ВКР)	Лица, оценивающие сформированность компетенций
1	2	3	4
		дителя 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-13	Текст ВКР	*Знать*: основные методы управления информационной безопасностью; методы аттестации уровня защищенности информационных систем; основные угрозы безопасности информации и модели нарушителя в информационных системах; принципы формирования политики информационной безопасности в информационных системах. *Уметь*: определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных систем. *Владеть*: навыками анализа информационной инфраструктуры информационной системы и ее безопасности; методами управления информационной безопасностью информационных систем.	Научный руководитель, рецензент
	Доклад на защите и презентация работы		Члены ГЭК
ПК-14	Текст ВКР	*Знать*: основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации; правовые основы организации защиты информации конфиденциального характера; организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения технической защиты информации конфиденциального характера, по аттестации объектов информатизации и сертификации средств защиты информации. *Уметь*: применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации. *Владеть*: навыками работы с нормативными правовыми актами; методами организации и управ-	Научный 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
		ления деятельностью служб защиты информации на предприятии; методами формирования требований по защите информации.	
ПК-15	Текст ВКР	*Знать*: принципы организации информационных систем в соответствии с требованиями по защите информации.	Научный руководитель, рецензент
	Ответы на вопросы членов ГЭК	*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.	Члены ГЭК
ПК-16	Текст ВКР	*Знать*: основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области. *Уметь*: разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации; составлять документы на любом носителе в зависимости от назначения, содержания и вида документа. *Владеть*: навыками работы с нормативными правовыми актами; навыками работы с документами.	Научный руководитель, рецензент
Дополнительные профессиональные компетенции			
ДПК-1	Текст ВКР	*Знать*: правовые и организационные основы системы транспортной безопасности; состав сил и средств обеспечения транспортной безопасности. *Уметь*: оценивать критерии и необходимость применения технических средств защиты информации на объектах транспортной инфраструктуры в зависимости от характеристик объекта защиты. *Владеть*: навыками анализа нормативных правовых документов в сфере транспортной безопасности.	Научный руководитель, рецензент
	Доклад на защите и презентация работы		Члены ГЭК

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

ПЛ 2.3.23-2018 «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 2.3.22–2018 «О формировании фонда оценочных материалов (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: 10.04.01
(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
2018

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 2019-2020 уч. год	ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №1 Государственный экзамен Направление подготовки магистров 10.04.01 «Информационная безопасность»	УТВЕРЖДАЮ: и.о. зав. каф. ИТиЗИ В. В. Башуров

1. Техническое задание на создание защищенных автоматизированных систем. Структура, порядок разработки (ГОСТ 34.602-89).
2. Подсистема отказоустойчивости, резервного копирования и восстановления информации.
3. Составляющая системы транспортной безопасности, направленная на обеспечение информационной безопасности.
4. Определите класс защищенности федеральной государственной информационной системы, если для конфиденциальности информации определена средняя степень ущерба, для целостности определена средняя степень ущерба и для доступности определена низкая степень ущерба.

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)

Отдел Докторантуры и Аспирантуры
Кафедра «Информационные технологии и защита информации»
Направление подготовки «Информационная безопасность»

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

Задание
на выпускную квалификационную работу обучающемуся

Гинановой Юлии Рашитовне
(Фамилия Имя Отчество)

1. Тема ВКР Разработка и внедрение правил антивирусной защиты и применение средств Антивируса Касперского для реализации параметров политики информационной безопасности Свердловской железной дороги
утверждена приказом по университету от «29» мая 2017г. № 1153-со
2. Срок сдачи обучающимся законченного ВКР 21 июня 2017
3. Исходные данные к ВКР: статистические данные угроз заражения через сеть Интернет и локальных, нормативные документы Свердловской железной дороги, руководства к средствам защиты от «Лаборатории Касперского».
4. Содержание расчетно-пояснительной записки (перечень подлежащих разработке вопросов): Исследование вредоносных программ и проведение анализа статистических данных угроз заражения, Разработка правил антивирусной защиты, Разработка инструкции по антивирусной защите на персональных ЭВМ на полигоне Свердловской железной дороги.
5. Перечень демонстрационно-графического материала (с точным указанием обязательных чертежей и другого наглядного материала): Цель работы; Особенности полигона Свердловской железной дороги; Структура серверов администрирования; Основные компоненты Kaspersky Security Center; Политика АВЗ для клиентских компьютеров; Оптимизация схемы размещения серверов администрировани; Заключение.

КАЛЕНДАРНЫЙ ПЛАН-ГРАФИК

№ п/п	Наименование этапов ВКР	Срок выполнения этапов ВКР	Примечание
1.	Утверждение темы диссертационного исследования	29.05.2017	
2.	Разработка плана исследования	30-31.05.2017	
3.	Подбор и изучение источников информации по теме ВКР	01-05.06.2017	
4.	Разработка ВКР в соответствии с планом	05-15.06.2017	
5.	Анализ и обобщение полученных результатов	15-17.06.2017	
6.	Оформление выпускной квалификационной работы	18-19.06.2017	
7.	Сдача ВКР на кафедру	20.06.2017	

Дата выдачи задания, руководитель

20.06.2017 _____
(дата, подпись ФИО)

Задание принял к исполнению обучающийся 20.06.17 _____ / Пинаева Ю.Р.
(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 2.3.23-2018 «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 2.3.23-2018 «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 2.3.22–2018 «О формировании фонда оценочных материалов (средств)».

Лист согласования фонда оценочных материалов государственной итоговой аттестации

Направление подготовки:

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

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

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

Протокол заседания кафедры № 1 от « 28 » августа 2018 г.

СОГЛАСОВАНО:

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

Лист согласования к программе государственной итоговой аттестации

Направление подготовки:

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

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

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

Протокол заседания кафедры № 1 от « 28 » августа 2018 г.

СОГЛАСОВАНО:

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