Минобрнауки России
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Сыктывкарский государственный университет имени Питирима Сорокина»
(ФГБОУ ВО «СГУ им. Питирима Сорокина»)

Утверждена
в составе Основной
профессиональной образовательной
программы высшего образования

ПРОГРАММА
ИТОГОВОЙ (ГОСУДАРСТВЕННОЙ ИТОГОВОЙ) АТТЕСТАЦИИ

Направление подготовки:

10.05.03 Информационная безопасность автоматизированных систем

Направленность (профиль) программы:

специализация N 7 "Анализ безопасности информационных систем"

Сыктывкар – 2025

1. Общие положения

Программа итоговой (государственной итоговой) аттестации разработана в соответствии с требованиями федерального государственного образовательного стандарта высшего образования (далее – ФГОС ВО) по направлению подготовки (специальности) 10.05.03 Информационная безопасность автоматизированных систем (утв. приказом Минобрнауки России от 26.11.2020 № 1457), и локальными актами университета.

Итоговая аттестация представляет собой форму оценки степени и уровня освоения обучающимися образовательной программы.

Итоговая (государственная итоговая) аттестация (далее – ГИА/ИА) проводится экзаменационными (государственными экзаменационными) комиссиями в целях определения соответствия результатов освоения обучающимися основных образовательных программ соответствующим требованиям федерального государственного образовательного стандарта (далее – ФГОС ВО).

В соответствии с ОПОП ГИА/ИА проверяет уровень сформированности универсальных, общепрофессиональных, профессиональных компетенций.

В соответствии с требованиями ФГОС ВО выпускник должен быть готов к решению задач (-и) профессиональной деятельности следующих (-его) типов (-а) в соответствии с ОПОП:

- научно-исследовательский
- проектный
- контрольно-аналитический
- организационно-управленческий
- эксплуатационный

Формы проведения итоговой (государственной итоговой) аттестации (далее вместе – итоговые (государственные) аттестационные испытания):

Подготовка к сдаче и сдача государственного экзамена

Подготовка к процедуре защиты и защита выпускной квалификационной работы

Общая трудоемкость итоговой (государственной итоговой) аттестации: 9 зачетных единиц.

2. Программа итоговой (государственной итоговой) аттестации: итоговый (государственный) экзамен

2.1. Цель и задачи итогового (государственного) экзамена.

Цель итогового (государственного) экзамена:

Комплексная оценка сформированности у выпускника профессиональных компетенций, необходимых для проектирования, реализации, эксплуатации и совершенствования систем защиты информации в автоматизированных системах, а также подтверждение его готовности к самостоятельной профессиональной деятельности в соответствии с требованиями ФГОС.

Задачи итогового (государственного) экзамена:

1. Верификация целостности профессионального мировоззрения

Проверить, способен ли выпускник к синтезу знаний из различных дисциплин (правовое обеспечение ИБ, сетевая безопасность, администрирование) для решения комплексной задачи.

2. Оценка способности к системному анализу и абстрактному мышлению

Определить, может ли выпускник перейти от частного случая к общей модели угроз и обратно. Экзамен должен ответить на вопрос: способен ли он, столкнувшись с конкретным инцидентом или уязвимостью, выявить системную проблему в архитектуре АС, а получив задачу спроектировать защиту, — предугадать частные векторы атак на свою конструкцию.

3. Аттестация способности к аргументированной защите своих решений

Проверить сформированность профессиональной уверенности и коммуникативной компетенции. Выпускник должен не только дать правильный ответ, но и грамотно его обосновать, отстоять свою точку зрения перед комиссией экспертов.

4. Подтверждение соответствия выпускника актуальному запросу рынка труда

Установить, что компетенции выпускника релевантны текущим и перспективным требованиям работодателей.

5. Формирование итоговой обратной связи для совершенствования образовательной программы

Получить диагностические данные о сильных и слабых сторонах подготовки студентов. Анализ ответов и типичных ошибок выпускников позволяет выявить пробелы в учебном плане, скорректировать содержание курсов, методы преподавания и расставить необходимые акценты в подготовке следующих поколений студентов.

Трудоемкость итоговой (государственной итоговой) аттестации в форме итогового (государственного) экзамена: 3 зачетных единиц.

Формы проведения итогового (государственного) экзамена:

- устно

2.2. Перечень дисциплин (модулей), формирующих программу итогового (государственного) экзамена

В программу итогового (государственного) экзамена включены вопросы и/или задания по дисциплинам (модулям), результаты освоения которых имеют определяющее значение для профессиональной деятельности выпускников:

- Безопасность операционных систем
- Угрозы информационной безопасности автоматизированных систем
- Моделирование систем и средств защиты информации
- Организационное и правовое обеспечение информационной безопасности
- Программно-аппаратные средства защиты информации
- Разработка и эксплуатация автоматизированных систем в защищенном исполнении

2.3. Содержание итогового (государственного) экзамена

Содержание итогового (государственного) экзамена включает наименование разделов и/или тем соответствующих дисциплин (модулей), результаты освоения которых имеют определяющее значение для профессиональной деятельности выпускников, либо могут представлять собой комплексные темы междисциплинарного характера.

Наименование разделов и/или тем, выносимых на итоговый (государственный) экзамен:

1. Безопасность операционных систем

Тема 1: Методы и средства усиления защищенности операционных систем (на примере ОС семейств Windows, Linux). Анализ политик безопасности, управления учетными записями и аудита.

Тема 2: Механизмы разграничения доступа в операционных системах: дискреционный, мандатный и ролевой подходы. Их сравнительный анализ, достоинства, недостатки и области применения.

2. Угрозы информационной безопасности автоматизированных систем

Тема 3: Классификация угроз информационной безопасности автоматизированных систем. Модели нарушителя. Источники, причины и цели реализации угроз.

Тема 4: Современные угрозы прикладного и системного программного обеспечения: уязвимости, вредоносное ПО, атаки типа "Zero-day". Методы и средства противодействия.

3. Моделирование систем и средств защиты информации

Тема 5: Формальные модели политик безопасности (Белла-ЛаПадулы, Биба, Кларка-Уилсона). Их назначение, принципы и практическая значимость при построении защищенных АС.

Тема 6: Методологии и технологии оценки рисков информационной безопасности. Качественные и количественные методы. Выбор и реализация мер по минимизации рисков.

4. Программно-аппаратные средства защиты информации

Тема 7: Средства криптографической защиты информации (СКЗИ): алгоритмы, протоколы, области применения. Назначение и функционирование инфраструктуры открытых ключей (PKI).

Тема 8: Межсетевые экраны и системы обнаружения и предотвращения вторжений (IDS/IPS). Принципы работы, архитектура размещения, достоинства и недостатки различных типов.

Тема 9: Технические средства защиты информации от утечки по каналам побочных электромагнитных излучений и наводок (ПЭМИН). Принципы действия и организация мероприятий по защите.

5. Организационное и правовое обеспечение информационной безопасности

Тема 10: Основные нормативно-правовые акты Российской Федерации в области информационной безопасности (ФЗ-152 "О персональных данных", ФЗ-187 "О безопасности КИИ", ФЗ-149 "Об информации..."). Ответственность за нарушения.

Тема 11: Разработка организационно-распорядительной документации по обеспечению ИБ. Политика безопасности, регламенты, инструкции для пользователей и администраторов.

Тема 12: Лицензирование деятельности и сертификация средств защиты информации в РФ. Порядок проведения и значимость для построения защищенных АС.

6. Разработка и эксплуатация автоматизированных систем в защищенном исполнении

Тема 13: Жизненный цикл защищенной автоматизированной системы. Требования по информационной безопасности на этапах проектирования, разработки, внедрения и эксплуатации.

Тема 14: Модель угроз и модель нарушителя для проектируемой автоматизированной системы. Методика их разработки и практическое использование при создании системы защиты.

Тема 15: Архитектура системы защиты информации автоматизированной системы. Принципы построения, выбор и интеграция различных средств защиты (технических, программных, организационных).

3. Учебная литература, ресурсы сети Интернет, программное обеспечение

- основная литература:

Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2021. — 312 с. — (Высшее

образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL:https://urait.ru/book/programmno-apparatnye-sredstva-zaschity-informacii-zaschita-programmnogo-obespecheniya-471159

Козырь, Н. С. Оценка рисков и аудит информационной безопасности : учебник для вузов / Н. С. Козырь, В. Н. Хализев. — Москва : Издательство Юрайт, 2025. — 190 с. — (Высшее образование). — ISBN 978-5-534-17864-7. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL:https://urait.ru/book/ocenka-riskov-i-audit-informacionnoy-bezopasnosti-581501

Грекул, В. И. Проектирование информационных систем : учебник и практикум для вузов / В. И. Грекул, Н. Л. Коровкина, Г. А. Левочкина. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 404 с. — (Высшее образование). — ISBN 978-5-534-19505-7. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL:https://urait.ru/book/proektirovanie-informacionnyh-sistem-560976

Зенков, А. В. Информационная безопасность и защита информации : учебник для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL:https://urait.ru/book/informacionnaya-bezopasnost-i-zaschita-informacii-567915

Гостев, И. М. Операционные системы : учебник и практикум для вузов / И. М. Гостев. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2025. — 164 с. — (Высшее образование). — ISBN 978-5-534-04520-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL:https://urait.ru/book/operacionnye-sistemy-561557

Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2025. — 424 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL:https://urait.ru/book/kriptograficheskie-metody-zaschity-informacii-dlya-izuchayuschih-kompyuternuyu-bezopasnost-560426

- дополнительная литература:

- периодические издания и реферативные базы данных (при необходимости):

ИВИС : универсальные базы электронных периодических изданий : сайт / ООО «ИВИС». – URL: https://dlib.eastview.com . – Режим доступа: для авториз. пользователей.

- электронно-библиотечные системы:

ЮРАЙТ : электронно-библиотечная система : сайт / ООО «Электронное издательство ЮРАЙТ». - URL:https://urait.ru/. Режим доступа: для авториз.пользователей

- современные профессиональные базы данных:

- информационные справочные системы:

Справочно-правовая информационная система Консультант Плюс http://www.consultant.ru/.

- лицензионное и свободно распространяемое программное обеспечение:

операционная система Windows, офисный пакет, текстовые и графические редакторы, программы для просмотра документов, браузеры.

2.5. Фонд оценочных средств итоговой (государственной итоговой) аттестации: итоговый (государственный) экзамен

2.5.1. Перечень компетенций и критерии оценки результатов сдачи итогового (государственного) экзамена.

В рамках проведения итогового (государственного) экзамена проверяется сформированность следующих компетенций:

Содержание и шифр компетенции	Планируемые результаты обучения		
	Знать	Уметь	Владеть
УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	принципы сбора, отбора и обобщения информации	соотносить разнородные явления и систематизировать их в рамках избранных видов деятельности	способностью грамотно, логично, аргументированно формировать собственные суждения и оценки
УК-2 Способен управлять проектом на всех этапах его жизненного цикла	правовые нормы, необходимые для достижения поставленной цели при реализации проекта	определять круг задач в рамках избранных видов профессиональной деятельности, планировать собственную деятельность, исходя из имеющихся ресурсов, соотносить главное и второстепенное, решать поставленные задачи в рамках избранных видов профессиональной деятельности	навыками отбора оптимальных технологий целедостижения; навыками работы с нормативными документами
УК-3 Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения	различные приёмы и способы социализации личности и социального взаимодействия	строить отношения с окружающими людьми, с коллегами	способностью определять свою роль в команде на основе использования стратегии сотрудничества для достижения

поставленной цели			поставленной цели
УК-4 Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	основы коммуникации, нормы, правила и особенности её осуществления в устной и письменной формах на русском и иностранном(ых) языке(ах)	применять правила и нормы деловой коммуникации на русском и иностранном(ых) языке(ах)	навыками применения коммуникативных технологий на русском и иностранном(ых) языке(ах) для академического и профессионального взаимодействия
УК-5 Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	основные категории философии, законы исторического развития, основы межкультурной коммуникации	анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	навыками коммуникации с представителями иных национальностей и конфессий с соблюдением этических и межкультурных норм
УК-6 Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни	основные принципы самовоспитания и самообразования, профессионального и личностного развития, исходя из этапов карьерного роста и требований рынка труда	планировать своё рабочее время и время для саморазвития, формулировать цели личностного и профессионального развития и условия их достижения, исходя из тенденций развития области профессиональной деятельности, индивидуально-личностных особенностей	выстраивать траекторию саморазвития посредством обучения по дополнительным образовательным программам
УК-7 Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности	основы здорового образа жизни, здоровьесберегающих технологий, физической культуры	выполнять комплекс физкультурных упражнений	практический опыт занятий физической культурой
УК-8 Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов	основы безопасности жизнедеятельности, телефоны служб спасения	оказать первую помощь в чрезвычайных ситуациях, создавать безопасные условия реализации профессиональной деятельности	навыками поддержания безопасных условий жизнедеятельности
УК-9 Способен принимать обоснованные экономические решения в различных областях	базовые принципы функционирования экономики и экономического развития, цели и формы участия	применять методы личного экономического и финансового планирования для достижения текущих и	инструментами управления личными финансами для достижения поставленных

жизнедеятельности	государства в экономике	долгосрочных финансовых целей, использует финансовые инструменты для управления личными финансами (личным бюджетом), контролирует собственные экономические и финансовые риски	финансовых целей
УК-10 Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	природу коррупции как социально-правового явления, общественную опасность коррупции во всех её проявлениях, её последствия и необходимость противодействия ей	толковать нормативные правовые акты антикоррупционной направленности; обнаруживать признаки антикоррупционных правонарушений и давать им общую правовую оценку; в рамках закона противодействовать коррупционным проявлениям	навыками реализации положений антикоррупционного законодательства
ОПК-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;	основные понятия информатики; назначение, функции и структуру операционных систем, вычислительных сетей и систем управления базами данных.	использовать программные и аппаратные средства персонального компьютера; применять программные средства системного, прикладного и специального назначения	навыками поиска информации в глобальной информационной сети Интернет и работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов, СУБД и т.п.); навыками обеспечивать работоспособности операционных систем и прикладных программ
ОПК-2 Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности;	основные информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства и методы использования.	применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства	навыками решения задач профессиональной деятельности с использованием информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства.
ОПК-3 Способен использовать математические методы, необходимые для решения задач профессиональной деятельности;	необходимые математические методы.	определять и применять необходимые математические методы	навыками решения задач профессиональной деятельности с использованием необходимых математических методов

ОПК-4 Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности;	физические законы и модели, в так же явления и процессы, лежащие в основе функционирования микроэлектронной техники	определять и применять необходимые физические законы и модели при решении задач профессиональной деятельности	навыками решения задач профессиональной деятельности с использованием необходимых физических законов и моделей
ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;	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; основные нормативные правовые акты в области информационной безопасности и защиты информации	применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; пользоваться нормативными документами по защите информации - пользоваться нормативными документами по защите информации.	навыками работы с нормативными правовыми актами; навыками работы с нормативными правовыми актами по защите информации
ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	правовые основы организации защиты государственной тайны и конфиденциальной информации; задачи органов защиты государственной тайны и служб защиты информации на предприятиях; организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации; нормативные методические документы ФСБ России, ФСТЭК России в области защиты информации	пользоваться нормативными документами ФСБ России и ФСТЭК России в области защиты информации	навыками организации и обеспечения режима коммерческой тайны и/или режима секретности.
ОПК-7 Способен создавать программы на языках общего назначения, применять методы и инструментальные	современные средства разработки и анализа программного обеспечения на языках высокого уровня; методы программирования и	выбирать необходимые инструментальные средства для разработки программ в различных операционных системах и средах; составлять,	навыками разработки программ на языке программирования высокого уровня; основными подходами к организации процесса

средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ;	методы разработки эффективных алгоритмов решения прикладных задач	тестировать, отлаживать и оформлять программы на языках высокого уровня, включая объектно-ориентированные	разработки программного обеспечения
ОПК-8 Способен применять методы научных исследований при проведении разработок в области защиты информации в автоматизированных системах;	основные методы поиска информации по ключевым словам; основные источники информации по вопросам обеспечения информационной безопасности	осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по профилю своей деятельности; составлять обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности	навыками представления результатов научных исследований по вопросам обеспечения информационной безопасности по профилю своей деятельности с использованием современных технических средств в устной и письменной формах
ОПК-9 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации;	современные информационные технологии и средства технической защиты информации, сетей и систем передачи информации, основные тенденции их развития	выявлять тенденции развития информационных технологий	навыками решения задач профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации
ОПК-10 Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности;	современные средства криптографической и технической защиты информации	использовать и настраивать современные средства криптографической и технической защиты информации	навыками решения задач профессиональной деятельности с использованием современных средства криптографической и технической защиты информации
ОПК-11 Способен разрабатывать компоненты систем защиты информации автоматизированных систем;	структуру систем защиты информации автоматизированных систем.	выявлять основные компоненты системы защиты информации автоматизированных систем	навыками разработки компонентов систем защиты защиты информации автоматизированных систем
ОПК-12 Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем;	основные подходы к обеспечению безопасности вычислительных сетей, операционных систем и баз данных	настраивать компоненты и средства защиты информации для вычислительных сетей, операционных систем и баз данных	навыками обеспечения безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем
ОПК-13 Способен организовывать и проводить диагностику	методы диагностики и тестирования систем защиты информации	применять средства диагностики и тестирования систем	навыками диагностики и тестирования систем защиты информации

и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем;	автоматизированных систем, методы анализа уязвимостей систем защиты информации автоматизированных систем	защиты информации автоматизированных систем, средства анализа уязвимостей систем защиты информации автоматизированных систем	автоматизированных систем, способен проводить анализ уязвимостей систем защиты информации автоматизированных систем
ОПК-14 Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений;	требования законодательства к защите информации в автоматизированных системах	проводить подготовку исходных данных для технико-экономического обоснования проектных решений для систем защиты информации в автоматизированных системах	навыками разработки, внедрения и эксплуатации автоматизированных систем в защищённом исполнении с учетом требований по защите информации
ОПК-15 Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем;	методы администрирования и контроля функционирования средств и систем защиты информации автоматизированных систем, методы инструментального мониторинга защищенности автоматизированных систем	применять средства администрирования и контроля функционирования средств и систем защиты информации автоматизированных систем, применять средства инструментального мониторинга защищенности автоматизированных систем	навыками администрирования и контроля функционирования средств и систем защиты информации автоматизированных систем, навыками инструментального мониторинга защищенности автоматизированных систем
ОПК-16 Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма.	основные закономерности исторического процесса; этапы исторического развития России, место и роль России в истории человечества и в современном мире; ключевые события истории России и мира с древности до наших дней, выдающихся деятелей отечественной истории; различные оценки и периодизации Отечественной истории	соотносить общие исторические процессы и отдельные факты, выявлять существенные черты исторических процессов, явлений и событий; извлекать уроки из исторических событий и на их основе принимать осознанные решения; осуществлять эффективный поиск информации и критику источников; получать, обрабатывать и сохранять источники информации; формулировать и аргументировано отстаивать собственную позицию по различным проблемам истории	представлениями о событиях российской и всемирной истории, основанными на принципе историзма; навыками анализа исторических источников; приёмами ведения дискуссии и полемики
ОПК-7.1. Способен использовать программные и программно-аппаратные средства для	подходы к моделированию и испытанию систем защиты информации информационных систем	использовать программные и программно-аппаратные средства для моделирования систем	навыками использования программных и программно-аппаратных средства для

моделирования и испытания систем защиты информационных систем;		защиты информационных систем	моделирования и испытания систем защиты информационных систем
ОПК-7.2. Способен разрабатывать методики и тесты для анализа степени защищенности информационной системы и ее соответствия нормативным требованиям по защите информации;	нормативные требования по защите информации информационных систем	разрабатывать методики для анализа защищенности информационных систем	навыками разработки методики и тестов для анализа степени защищенности информационной системы и ее соответствия нормативным требованиям по защите информации
ОПК-7.3. Способен проводить анализ защищенности и верификацию программного обеспечения информационных систем;	методы анализа защищенности и верификации программного обеспечения	проводить анализ защищенности и верификацию программного обеспечения	навыками анализа защищенности и верификации программного обеспечения информационных систем
ПК-1 Обеспечение информационной безопасности компьютерных систем и сетей	основные подходы к обеспечению информационной безопасности компьютерных систем и сетей.	настраивать компьютерные системы и сети в соответствии с требованиями по обеспечению информационной безопасности	навыками обеспечения информационной безопасности компьютерных систем и сетей
ПК-2 Разработка систем защиты информации автоматизированных систем	основные требования нормативных документов в области защиты информации в автоматизированных системах; знает основные подходы к разработке систем защиты информации автоматизированных систем.	разрабатывать проекты систем защиты информации автоматизированных систем	навыками разработки систем защиты информации автоматизированных систем.
ПК-3 Формирование требований к защите информации в автоматизированных системах	требования законодательства к защите информации в автоматизированных системах; знает подходы к формированию требований по защите информации в автоматизированных системах	формировать требования к защите информации в автоматизированных системах на основании нормативных документов	навыками формирования требований к защите информации в автоматизированных системах на основании анализа и моделирования системы защиты информации
ПК-4 Организация и проведение работ по технической защите информации	основы организации работы коллектива и методы принятия управленческих решений	применять методы принятия управленческих решения для организации работы коллектива в профессиональной деятельности	навыками организации и проведения работ по технической защите информации для обеспечения информационной безопасности автоматизированных систем.
ПК-5 Проведение аттестации объектов на	положения нормативных документов по аттестации	проводить контроль защищенности	навыками проведения аттестации

соответствие требованиям по защите информации	объектов информатизации	автоматизированной системы от утечки по техническим каналам и от НСД к информации	автоматизированных систем на соответствие требованиям по защите информации

2.5.2. Оценочные средства:

Перечень вопросов и/или заданий, выносимых на итоговый (государственный) экзамен:

I. Безопасность операционных систем

Модели управления доступом в операционных системах: дискреционный, мандатный, ролевой.

Механизмы аутентификации в ОС Windows: архитектура, уязвимости и методы усиления.

Подсистема безопасности Linux (SELinux, AppArmor): принципы работы и настройка.

Безопасность виртуализированных сред: архитектура и угрозы.

Аудит и мониторинг событий безопасности в операционных системах.

Защита памяти ОС: ASLR, DEP, защита кучи.

Безопасность системных служб и привилегированных учетных записей.

Обновление и исправление ОС: процессы управления патчами.

Безопасная настройка и hardening ОС семейств Windows и Linux.

Изоляция процессов и контейнеров как механизм безопасности.

II. Угрозы информационной безопасности автоматизированных систем

11. Классификация угроз ИБ по источникам, способам реализации и последствиям.

12. Угрозы сетевой безопасности: классификация и примеры атак.

13. Социальная инженерия как угроза ИБ: методы и способы защиты.

14. Угрозы безопасности веб-приложений (OWASP Top 10).

15. Атаки на криптографические алгоритмы и протоколы.

16. Угрозы безопасности интернета вещей (IoT).

17. Целевые атаки (APT): характеристики и жизненный цикл.

18. Угрозы безопасности облачных сред.

19. Вредоносное ПО: классификация, способы распространения и методы обнаружения.

20. Уязвимости программного обеспечения: классификация и процесс управления.

III. Моделирование систем и средств защиты информации

21. Формальные модели политик безопасности (Белла-ЛаПадулы, Биба, Кларка-Уилсона).

22. Модели управления доступом на основе ролей (RBAC).

23. Методологии оценки рисков ИБ: качественные и количественные методы.

24. Построение моделей угроз для автоматизированных систем.

25. Моделирование инцидентов информационной безопасности.

26. Критерии оценки безопасности информационных систем.

27. Модели обеспечения целостности информации.

28. Формальные методы верификации систем защиты.

29. Моделирование процессов управления доступом в распределенных системах.

30. Системы управления информационной безопасностью (СУИБ).

IV. Программно-аппаратные средства защиты информации

31. Архитектура и типы межсетевых экранов.

32. Системы обнаружения и предотвращения вторжений (IDS/IPS).

33. Средства криптографической защиты информации: классификация и применение.

34. Системы управления ключами и сертификатами (PKI).

35. Технические средства защиты от утечки по каналам ПЭМИН.

36. Системы резервного копирования и восстановления данных.

37. Аппаратные модули доверенной загрузки.

38. Средства контроля целостности информации.

39. Системы защиты от DDoS-атак.

40. Средства анализа защищенности (сканеры уязвимостей).

V. Организационное и правовое обеспечение информационной безопасности

41. Законодательство РФ в области ИБ: основные законы и требования.

42. Лицензирование деятельности и сертификация СЗИ в РФ.

43. Политика информационной безопасности: структура и содержание.

44. Организационные меры защиты персональных данных.

45. Регламенты реагирования на инциденты ИБ.

46. Требования к безопасности критической информационной инфраструктуры.

47. Международные стандарты в области ИБ (ISO 27000).

48. Аудит и сертификация систем защиты информации.

49. Правовые аспекты использования электронной подписи.

50. Ответственность за правонарушения в области ИБ.

2.5.3. Критерии оценивания результатов сдачи итогового (государственного) экзамена:

Критерии оценивания	
отлично	обучающийся способен самостоятельно искать, анализировать и оценивать профессиональную информацию; понимать методологические основы профессиональной деятельности; решать различные типы практических задач в профессиональной области, в том числе корректировать свои действия при изменении условий выполнения задачи, а также в различных рабочих ситуациях; осуществлять текущий и итоговый контроль своей, а при необходимости и групповой профессиональной деятельности, ее оценку и при необходимости коррекцию; принимать решения в сфере исполнения своих обязанностей; проявлять полученные навыки при решении профессиональных задач различной сложности; избирать пути решения сложных профессиональных задач. При ответе на вопросы и/или выполнении заданий обучающийся обнаруживает всестороннее и глубокое знание программного материала; использует соотносимые знания дисциплин, не включенных в программу экзамена; демонстрирует знание современной учебной и научной литературы; точно и корректно использует научную и специальную терминологию; стилистически грамотно, логически правильно излагает ответы на вопросы билета и дополнительные вопросы; обнаруживает способность творчески применять знания теории к решению профессиональных задач; демонстрирует способность к комплексному анализу, сопоставлению различных подходов к рассмотрению вопросов и/или заданий билета, формулированию обоснованных выводов, умение ориентироваться в теориях, концепциях и направлениях по проблематике вопросов, давать им критическую оценку, использовать научные достижения других дисциплин;
хорошо	обучающийся способен самостоятельно искать, анализировать и оценивать профессиональную информацию; решать различные типы практических задач в профессиональной области, в том числе корректировать свои действия при изменении условий выполнения задачи; осуществлять текущий и итоговый контроль своей профессиональной деятельности, ее оценку и при необходимости коррекцию; владеет сложными навыками в сфере своей профессиональной деятельности, способен, используя их, активно влиять на происходящее, самостоятельно принимать решения в сфере профессиональной деятельности и проявлять полученные навыки в ситуациях различной сложности. При ответе на вопросы и/или выполнении заданий обучающийся обнаруживает всестороннее систематическое и глубокое знание программного материала в целом; использует при ответе соотносимые знания дисциплин, не включенных в программу экзамена; демонстрирует знание современной учебной и научной литературы; корректно использует научную и специальную терминологию; стилистически грамотно, логически правильно излагает ответы на вопросы билета и дополнительные вопросы; обнаруживает

	способность применять знания теории к решению профессиональных задач; демонстрирует способность к комплексному анализу вопросов и/или заданий билета и формулированию обоснованных выводов, умение в целом ориентироваться в теориях, концепциях и направлениях по проблематике вопросов, давать им критическую оценку; допускает отдельные погрешности и неточности в формулировках;
удовлетворительно	обучающийся имеет представление о том, какие именно способности должны сформироваться в процессе обучения по данному направлению; способен самостоятельно искать, анализировать и использовать профессиональную информацию; способен, используя полученные знания и навыки, самостоятельно на должном уровне осуществлять основные виды профессиональной деятельности, решать различные типы практических задач в профессиональной области, в том числе корректировать свои действия при изменении условий выполнения задачи, самостоятельно контролировать, оценивать и корректировать свою профессиональную деятельность. При ответе на вопросы и/или выполнении заданий обучающийся показывает достаточные знания отдельных блоков программного материала; демонстрирует фрагментарное знание современной учебной и научной литературы; корректно использует научную и специальную терминологию; стилистически грамотно, логически правильно излагает ответы на вопросы билета и дополнительные вопросы; обнаруживает способность применять знания теории к решению профессиональных задач; демонстрирует способность к формулированию выводов, умение в целом ориентироваться в основных теориях, концепциях и направлениях по проблематике вопросов, давать им сравнительную оценку; допускает существенные погрешности и неточности в формулировках;
неудовлетворительно	обучающийся не владеет необходимыми для осуществления профессиональной деятельности знаниями и навыками, или владеет ими фрагментарно, не способен их применять в процессе профессиональной деятельности, не способен решать типовые профессиональные задачи. При ответе на вопросы и/или выполнении заданий обучающийся показывает недостаточный объём знаний вопросов билета и программного материала в целом либо не дает ответ или отказывается от ответа хотя бы на один вопрос билета; не демонстрирует знание современной учебной и научной литературы; некорректно использует научную и специальную терминологию; излагает ответы на вопросы с существенными лингвистическими и логическими ошибками; обнаруживает некомпетентность в решении стандартных (типовых) профессиональных задач, неспособность к формулированию выводов; демонстрирует неумение ориентироваться в основных теориях, концепциях и направлениях по проблематике вопросов; допускает грубые стилистические и логические ошибки.

2.6. Методические материалы для итогового (государственного) экзамена

Рекомендации обучающемуся по подготовке к итоговому (государственному) экзамену:

1. Планирование подготовки

Получить и проанализировать официальную программу экзамена.

Провести диагностику знаний по экзаменационным темам.

Составить индивидуальный график подготовки с акцентом на проблемные разделы.

2. Организация работы с материалами

Использовать приоритетно: учебные программы, конспекты лекций, рекомендованную литературу.

Изучать нормативные документы (ФЗ-152, ФЗ-187, руководящие документы ФСТЭК).

Систематизировать информацию по темам с выделением: определений, классификаций, принципов работы, областей применения.

3. Формирование структуры ответов

Подготовить шаблоны ответов по каждому вопросу программы.

Включать в ответы: теоретические положения, практические примеры, сравнительный анализ.

Устанавливать междисциплинарные связи между различными разделами программы.

4. Развитие профессиональных компетенций

Акцент на понимание принципов и методологий, а не на механическое запоминание.

Тренировка навыков аргументации и решения комплексных задач.

Подготовка к вопросам по практическому применению теоретических знаний.

5. Контроль готовности

Регулярное самопроверка по ключевым положениям программы.

Участие в пробных экзаменах и групповых обсуждениях.

Анализ типовых ошибок и устранение выявленных пробелов.

6. Заключительный этап

Повторение ключевых понятий и схем взаимодействия.

Изучение дополнительных материалов по проблемным темам.

Обеспечение режима отдыха и психологической готовности к экзамену.

3. Программа итоговой (государственной итоговой) аттестации: выпускная квалификационная работа

3.1. Цель и задачи выпускной квалификационной работы

Цель выпускной квалификационной работы:

Цель заключается в демонстрации способности выпускника к самостоятельному решению комплексной задачи в области проектирования, реализации или оценки систем защиты информации, соответствующей требованиям федеральных государственных образовательных стандартов и профессиональной деятельности. Конкретные аспекты цели: - Систематизация и углубление профессиональных знаний в области защиты автоматизированных систем. - Разработка и обоснование практических решений по обеспечению информационной безопасности для конкретной предметной области. - Апробация методов и инструментов анализа угроз, моделирования рисков и проектирования систем защиты. - Оценка эффективности предложенных решений с учетом нормативно-правовых, технических и организационных требований. - Демонстрация готовности к профессиональной деятельности через решение актуальной задачи, соответствующей профилю направления.

Задачи выпускной квалификационной работы:

1. Демонстрация системного подхода к решению профессиональных задач

Показать способность анализировать, проектировать и реализовывать комплексные решения в области информационной безопасности

Обеспечить взаимосвязь теоретических знаний с практическими аспектами защиты автоматизированных систем

2. Подтверждение уровня сформированности профессиональных компетенций

Продемонстрировать владение методами и инструментами обеспечения информационной безопасности

Показать умение работать с нормативно-технической документацией и профессиональными стандартами

3. Апробация навыков исследования и проектирования

Реализовать полный жизненный цикл проекта - от анализа требований к защите до внедрения и оценки эффективности

Показать способность к критическому анализу и выбору оптимальных решений

4. Верификация готовности к самостоятельной профессиональной деятельности

Продемонстрировать умение формулировать и аргументировать технические решения

Показать способность нести ответственность за результаты проектной деятельности

5. Формирование основы для дальнейшего профессионального развития

Создать задел для последующей научно-исследовательской или практической работы

Показать потенциал для профессионального роста и адаптации к изменяющимся условиям

Трудоемкость итоговой (государственной итоговой) аттестации в форме защиты выпускной квалификационной работы: 6 зачетных единиц.

3.2. Темы выпускных квалификационных работ

Темы выпускных квалификационных работ соответствуют современному уровню развития науки, требованиям к уровню знаний и компетенций, имеют актуальность и практическую значимость и выполняются по предложению вуза, организаций и предприятий, научно-исследовательских и творческих коллективов и др.

По письменному заявлению обучающегося (нескольких обучающихся, выполняющих выпускную квалификационную работу совместно) университет в установленном порядке предоставляет обучающемуся (обучающимся) возможность подготовки и защиты выпускной квалификационной работы по теме, предложенной обучающимся (обучающимися), в случае обоснованности целесообразности ее разработки для практического применения в соответствующей области профессиональной деятельности или на конкретном объекте профессиональной деятельности.

Перечень тем выпускных квалификационных работ:

1. Использование методов и подходов форензики для обеспечения информационной безопасности.

2. Методы юридически значимого анализа инцидентов информационной безопасности.

3. Разработка методики обнаружения вредоносной активности в «интернете вещей» (IoT).

4. Обеспечение информационной безопасности «интернета вещей» (IoT).

5. Методы обеспечения безопасности «интернета вещей» (IoT).

6. Использование особенностей IP-протокола для построения стеганографических схем.

7. Разработка предложений по контент-анализу данных социальных сетей.

8. Разработка предложений по защите мультимедийной продукции от несанкционированного копирования.

9. Разработка модуля обнаружения вредоносного программного обеспечения в сетевом трафике по сигнатурам.

10. Разработка метода защиты графических изображений от встраивания вредоносной информации стеганографическими средствами.

11. Исследование методов оптимизации программных реализаций алгоритмов, применяемых для обеспечения информационной безопасности.

12. Исследование вопросов безопасности применения различных сред разработки программного обеспечения.

13. Разработка механизмов защиты информации для операционной системы Android.

14. Выявление уязвимостей защиты на установку и эксплуатацию вредоносного ПО Andoid OS.

15. Выявление уязвимостей защиты на установку и эксплуатацию вредоносного ПО iOS.

16. Разработка универсального сканера уязвимости защиты сервера и сети.

17. Ускорение криптографических вычислений путем низкоуровневых оптимизаций базовых блоков алгоритмов.

18. Разработка методики оценки защищенности информации по ИК-каналу.

19. Организация обеспечения информационной безопасности в организации.

20. Аналитические исследования технических каналов утечки информации.

21. Применение искусственного интеллекта в сфере обеспечения информационной безопасности.

22. Обеспечение безопасности web-приложений.

23. Применение CASE-подходов для обучения сотрудников организации принципам информационной безопасности.

24. Моделирование и разработка лаборатории имитации вредоносной активности и способов борьбы с ней.

25. Создание обучающего тренажера для специалистов в области информационной безопасности, согласно классификации OWASP.

26. Проведение тестирования на проникновение и выработка рекомендаций по устранению уязвимостей веб-сервера.

27. Обеспечение информационной безопасности в информационно-телекоммуникационных сетях с использованием объектно-ориентированного программирования.

28. Управление рисками для обеспечения информационной безопасности организации на основе информационно-аналитических систем управления знаниями.

29. Комплексное обеспечение информационной безопасности организации путем разработки автоматизированной системы аудита и реагирования на инциденты информационной безопасности.

30. Обеспечение ИБ организации с позиций информационной безопасности Российской Федерации и международной информационной безопасности.

31. Обеспечение информационной безопасности организации с использованием графовых информационно-аналитических систем и баз данных.

32. Обеспечение информационной безопасности объектов информатизации в условиях концепции «интернета вещей» (IoT).

33. Обеспечение информационной безопасности в информационно-телекоммуникационных сетях.

34. Обеспечение информационной безопасности организации на основе OSINT.

35. Обеспечение информационной безопасности CRM-систем.

36. Смарт-контракт и обеспечение его информационной безопасности.

37. Технология блокчейн и ее устойчивость с точки зрения ИБ: прикладные аспекты.

38. Цифровизация экономики в отраслевом разрезе: вопросы и проблемы обеспечения информационной безопасности.

39. Создание модели СЗИ и моделирование уровня защищенности на примере конкретного предприятия/организации.

40. Обеспечение информационной безопасности детей в сети Интернет.

41. Поведенческий анализ вредоносного программного обеспечения.

42. Обеспечение информационной безопасности функционирования предприятия малого бизнеса.

43. Создание лабораторного стенда «Хакинг системы».

44. Создание лабораторного стенда «Трояны и другое вредоносное ПО».

45. Разработка комплекса режимных мероприятий по сохранности сведений, составляющих государственную тайну в организации.

46. Учебно-методический комплекс по организации и ведению секретного делопроизводства.

47. Разработка рекомендаций по защите персональных данных на предприятии.

48. Контроль действий пользователей средствами DLP-системы.

49. Разработка методических рекомендаций по оценке эффективности экранированных заглушек в области ПЭМИН.

50. Обеспечение защиты информационно-телекоммуникационной сети (ИТКС) с помощью средств защиты информации (СЗИ).

51. Обеспечение информационной безопасности «клиента» на базе операционных систем Windows и Astra Linux.

52. Обеспечение информационной безопасности кибер-физических систем (CPS).

53. Обеспечение информационной безопасности при использовании систем электронного документооборота/ECM – систем в организации.

54. Обеспечение информационной безопасности при использовании облачных сервисов.

55. Обеспечение информационной безопасности фрагмента ИТКС с помощью сертифицированных решений компании Positive Technologies.

56. Применение аналитических подходов к обеспечению информационной безопасности организации.

57. Применение облачных технологий для оптимизации обучения в области информационной безопасности.

58. Организация защиты персональных данных в СГУ им. Питирима Сорокина.

59. Организация защиты конфиденциальной информации в СГУ им. Питирима Сорокина.

60. Обход систем обнаружения вторжений, фаерволов и Honeypot.

61. Разработка внутренней информационной системы по вопросам контроля осведомленности персонала в области информационной безопасности.

62. Создание модели киберполигона по обучению персонала навыкам обнаружения и противодействия угроз информационной безопасности.

63. Разработка тестового стенда для анализа и оптимизации основных параметров канала передачи данных от оконечного оборудования рубежа фотовидеофиксации.

64. Разработка системы мониторинга угроз информационной безопасности государственной информационной системы «Единая автоматизированная информационно-аналитическая система обеспечения деятельности ОГВ РК».

65. Разработка системы мониторинга угроз информационной безопасности государственной информационной системы «Государственная информационная система «Система обеспечения вызова экстренных оперативных служб по единому номеру «112» в Республике Коми».

66. Разработка модели системы защиты от потенциальных угроз информационной безопасности помещений директората ИТНИТ.

67. Разработка модели системы защиты информационной безопасности технической лаборатории на основе дискретной политики.

68. Разработка модели системы защиты информационной безопасности лаборатории от скрытых каналов.

69. Реверс-инжиниринг цифровых протоколов связи.

70. Исследование работы сетей сотовой связи 2-го поколения.

71. Разработка устройства для сетевого мониторинга на базе микрокомпьютера Raspberry Pi.

72. Разработка вычислительного кластера на базе микрокомпьютеров Raspberry Pi

73. Информационная безопасность встраиваемых вычислительных систем

74. Разработка устройства мониторинга радиоэфира с использованием технологии SDR.

75. Инструментальные средства разработки безопасного программного обеспечения.

76. Практические аспекты внедрения отечественного программного обеспечения в организации.

77. DevSecOps: обеспечение информационной безопасности на этапе разработки.

78. Обеспечение безопасности виртуальной инфраструктуры сертифицированными средствами на базе Linux.

79. Риски информационной безопасности в условиях импортозамещения.

80. Разработка сканера уязвимостей.

81. Обеспечение безопасности веб-приложений.

82. Выявление уязвимостей системы защиты.

83. Разработка механизмов защиты информации.

84. Разработка модуля обнаружения вредоносного программного обеспечения.

85. Разработка приложения по контент-анализу данных.

86. Фишинг и социальная инженерия.

87. Разработка модулей доверенной загрузки UEFI.

88. Разработка средства доверенной загрузки для порта M.2.

89. Автоматизация подготовки документов для аттестации объектов информатизации.

90. Автоматизация секретного делопроизводства на базе ОС Astra Linux Special Edition.

91. Оценка защищенности по каналу ПЭМИН: верификация опасных сигналов.

92. Разработка системы идентификации для ОС Linux на основе распознавания лица.

93. Восстановление речевого сигнала по нескольким измерениям в условиях шума.

94. Разработка программируемого имитатора закладных устройств.

95. Разработка модуля идентификации субъектов в сети Интернет

96. Валидация торрент-файлов на наличие вредоносной нагрузки

97. Разработка материалов для учебного практикума по информационной безопасности

98. Разработка системы выявления поддельных учетных записей в социальных сетях

99. Разработка и тестирование материалов учебного практикума на тему сбор информации, разведка и социальная инженерия

100. Разработка и тестирование материалов учебного практикума на тему сканирование сети и сниффинг

101. Разработка и тестирование материалов учебного практикума на тему анализ уязвимостей

102. Разработка и тестирование материалов учебного практикума на тему эксплуатация уязвимостей операционной системы

103. Разработка и тестирование материалов учебного практикума на тему вредоносное ПО

104. Разработка и тестирование материалов учебного практикума на тему перехват сеанса

105. Разработка и тестирование материалов учебного практикума на тестирование на проникновение веб-сервера

106. Разработка и тестирование материалов учебного практикума на тестирование на проникновение веб-приложения

107. Разработка и тестирование материалов учебного практикума на тему инъекций

108. Разработка и тестирование материалов учебного практикума на тему безопасности беспроводных сетей

109. Разработка метода оценки риска ИБ в киберфизических системах.

110. Применение оценки рисков ИБ в ERP системах

111. Разработка модели угроз ИБ в ERP системах

112. Применение оценки рисков ИБ в организациях государственного управления.

113. Применение оценки рисков ИБ в коммерческих организациях.

114. Разработка системы технического контроля эффективности мер защиты информации предприятия.

115. Разработка системы выявления технических каналов утечки информации предприятия.

116. Безопасность web-приложений

117. Защита данных Интернет-трафика путем реализации личного VPN-сервера

118. Внедрение SIEM системы в инфраструктуру предприятия

119. Аттестация помещений, объектов и средств вычислительной техники

120. Разработка межсетевого экрана для операционной системы Android

121. Организация информационной безопасности в процессах цифровой трансформации

122. Методы обеспечения информационной безопасности в процессах цифровой трансформации

123. Информационная безопасность мобильных приложений

124. Внедрение методов защиты информации при разработке ИС

125. Организация расследований инцидентов информационной безопасности

126. Разработка учебно-лабораторного комплекса к проведению соревнований по защите информации CTF

127. Организация технической защиты информации на предприятии

128. Разработка рекомендаций по организации внутреннего контроля за соответствием обработки персональных данных

129. Разработка методического комплекса по созданию подразделения по технической защите информации

130. Оценка реального затухания электромагнитные сигналов от ПЭВМ

131. ПЭМИН от видеоинтерфейсов СВТ: VGA, HDMI, DVI, Display Port

132. ПЭМИН от мониторов и дисплеев от линий LVDS, RSMS и eDP

133. Оценка ПЭМИН для ЛВС

3.3. Учебная литература, ресурсы сети Интернет, программное обеспечение

- основная литература:

Бушенева, Ю. И. Как правильно написать реферат, курсовую и дипломную работы : практическое пособие : [16+] / Ю. ;И. ;Бушенева. – Москва : Дашков и К°, 2016. – 140 с. : ил. – (Учебные издания для бакалавров). – Режим доступа: по подписке. – URL:https://biblioclub.ru/index.php?page=book&id=453258

Родионова, Д. Д. Основы научно-исследовательской работы (студентов) : учебное пособие : [16+] / Д. ;Д. ;Родионова, Е. ;Ф. ;Сергеева. – Кемерово : Кемеровский государственный университет культуры и искусств (КемГУКИ), 2010. – 181 с. – Режим доступа: по подписке. – URL:https://biblioclub.ru/index.php?page=book&id=227895

Сафронова, Т. Н. Основы научных исследований : учебное пособие / Т. ;Н. ;Сафронова, А. ;М. ;Тимофеева ; Сибирский федеральный университет. – Красноярск : Сибирский федеральный университет (СФУ), 2015. – 131 с. : табл., ил. – Режим доступа: по подписке. – URL:https://biblioclub.ru/index.php?page=book&id=435828

Основы научных и экспериментальных исследований в области информационной безопасности [Электронный ресурс] : учебное пособие / сост.: Л.С. Носов, Н.Р. Оленева, А.Н. Некрасов. - Сыктывкар : Изд-во СГУ им. Питирима Сорокина, 2018. - 66 с. URL:http://e-library.syktsu.ru/megapro/Download/MObject/704/Оленева Н.Р. Основы научных и экспериментальных исследований.pdf

- дополнительная литература:

- периодические издания и реферативные базы данных (при необходимости):

ИВИС : универсальные базы электронных периодических изданий : сайт / ООО «ИВИС». – URL: https://dlib.eastview.com . – Режим доступа: для авториз. пользователей.

- электронно-библиотечные системы:

– Университетская библиотека онлайн : электронно-библиотечная система : сайт / ООО «НексМедиа». – URL:https://biblioclub.ru. – Режим доступа: для авториз. пользователей.

- современные профессиональные базы данных:

- информационные справочные системы:

Справочно-правовая информационная система Консультант Плюс http://www.consultant.ru/.

- лицензионное и свободно распространяемое программное обеспечение:

операционная система Windows, офисный пакет, текстовые и графические редакторы, программы для просмотра документов, браузеры.

3.4. Фонд оценочных средств итоговой (государственной итоговой) аттестации: выпускная квалификационная работа

3.4.1. Перечень компетенций, сформированность которых проверяется по результатам защиты выпускной квалификационной работы.

В рамках выполнения выпускной квалификационной работы проверятся сформированность у выпускника следующих компетенций:

Содержание и шифр компетенции	Планируемые результаты обучения		
	Знать	Уметь	Владеть
УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	принципы сбора, отбора и обобщения информации	соотносить разнородные явления и систематизировать их в рамках избранных видов деятельности	способностью грамотно, логично, аргументированно формировать собственные суждения и оценки
УК-2 Способен управлять проектом на всех этапах его жизненного цикла	правовые нормы, необходимые для достижения поставленной цели при реализации проекта	определять круг задач в рамках избранных видов профессиональной деятельности, планировать собственную деятельность, исходя из имеющихся ресурсов, соотносить главное и второстепенное, решать поставленные задачи в рамках избранных видов профессиональной деятельности	навыками отбора оптимальных технологий целедостижения; навыками работы с нормативными документами
УК-3 Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	различные приёмы и способы социализации личности и социального взаимодействия	строить отношения с окружающими людьми, с коллегами	способностью определять свою роль в команде на основе использования стратегии сотрудничества для достижения поставленной цели
УК-4 Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	основы коммуникации, нормы, правила и особенности её осуществления в устной и письменной формах на русском и иностранном(ых) языке(ах)	применять правила и нормы деловой коммуникации на русском и иностранном(ых) языке(ах)	навыками применения коммуникативных технологий на русском и иностранном(ых) языке(ах) для академического и профессионального взаимодействия
УК-5 Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	основные категории философии, законы исторического развития, основы межкультурной коммуникации	анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	навыками коммуникации с представителями иных национальностей и конфессий с соблюдением этических и межкультурных норм
УК-6 Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни	основные принципы самовоспитания и самообразования, профессионального и личностного развития, исходя из этапов карьерного роста и требований рынка труда	планировать своё рабочее время и время для саморазвития, формулировать цели личностного и профессионального развития и условия их достижения, исходя из тенденций развития	выстраивать траекторию саморазвития посредством обучения по дополнительным образовательным программам

		области профессиональной деятельности, индивидуально-личностных особенностей	
УК-7 Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности	основы здорового образа жизни, здоровье-сберегающих технологий, физической культуры	выполнять комплекс физкультурных упражнений.	Имеет практический опыт занятий физической культурой
УК-8 Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов	основы безопасности жизнедеятельности, телефоны служб спасения	оказать первую помощь в чрезвычайных ситуациях, создавать безопасные условия реализации профессиональной деятельности	навыками поддержания безопасных условий жизнедеятельности
УК-9 Способен принимать обоснованные экономические решения в различных областях жизнедеятельности	базовые принципы функционирования экономики и экономического развития, цели и формы участия государства в экономике	применять методы личного экономического и финансового планирования для достижения текущих и долгосрочных финансовых целей, использует финансовые инструменты для управления личными финансами (личным бюджетом), контролирует собственные экономические и финансовые риски	инструментами управления личными финансами для достижения поставленных финансовых целей
УК-10 Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	природу коррупции как социально-правового явления. Понимает общественную опасность коррупции во всех ее проявлениях, ее последствия и необходимость противодействия ей	толковать нормативные правовые акты антикоррупционной направленности; обнаруживать признаки антикоррупционных правонарушений и давать им общую правовую оценку; в рамках закона противодействовать коррупционным проявлениям	навыками реализации положений антикоррупционного законодательства
ОПК-1 Способен оценивать роль	основные понятия информатики;	использовать программные и	навыками поиска информации в

информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;	назначение, функции и структуру операционных систем, вычислительных сетей и систем управления базами данных	аппаратные средства персонального компьютера; применять программные средства системного, прикладного и специального назначения	глобальной информационной сети Интернет и работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов, СУБД и т.п.); навыками обеспечивать работоспособности операционных систем и прикладных программ
ОПК-2 Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности;	основные программные средства системного и прикладного назначения, в том числе отечественного производства и методы использования	применять программные средства системного и прикладного назначения, в том числе отечественного производства	навыками решения задач профессиональной деятельности с использованием программных средств системного и прикладного назначения, в том числе отечественного производства
ОПК-3 Способен использовать математические методы, необходимые для решения задач профессиональной деятельности;	необходимые математические методы	определять и применять необходимые математические методы	навыками решения задач профессиональной деятельности с использованием необходимые математические методы
ОПК-4 Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности;	физические законы и модели, в так же явления и процессы, лежащие в основе функционирования микроэлектронной техники	определять и применять необходимые физические законы и модели при решении задач профессиональной деятельности	навыками решения задач профессиональной деятельности с использованием необходимых физических законов и моделей
ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;	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; основные	применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; пользоваться нормативными документами по защите информации	навыками работы с нормативными правовыми актами; навыками работы с нормативными правовыми актами по защите информации

	нормативные правовые акты в области информационной безопасности и защиты информации		
ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	правовые основы организации защиты государственной тайны и конфиденциальной информации; задачи органов защиты государственной тайны и служб защиты информации на предприятиях; организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации; нормативные методические документы ФСБ России, ФСТЭК России в области защиты информации	пользоваться нормативными документами ФСБ России и ФСТЭК России в области защиты информации	навыками организации и обеспечения режима коммерческой тайны и/или режима секретности
ОПК-7 Способен создавать программы на языках общего назначения, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ;	современные средства разработки и анализа программного обеспечения на языках высокого уровня; методы программирования и методы разработки эффективных алгоритмов решения прикладных задач	выбирать необходимые инструментальные средства для разработки программ в различных операционных системах и средах; составлять, тестировать, отлаживать и оформлять программы на языках высокого уровня, включая объектно-ориентированные	навыками разработки программ на языке программирования высокого уровня; основными подходами к организации процесса разработки программного обеспечения
ОПК-8 Способен применять методы научных исследований при проведении разработок в области защиты информации в автоматизированных системах;	основные методы поиска информации по ключевым словам; основные источники информации по вопросам обеспечения информационной безопасности автоматизированных систем	осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по профилю своей деятельности; составлять обзор по вопросам обеспечения информационной безопасности автоматизированных систем	навыками представления результатов научных исследований по вопросам обеспечения информационной безопасности по профилю своей деятельности с использованием современных технических средств в устной и письменной формах
ОПК-9 Способен решать задачи	современные информационные	выявлять тенденции развития	навыками решения задач профессиональной

профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации;	технологии и средства технической защиты информации, сетей и систем передачи информации, основные тенденции их развития	информационных технологий	деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации
ОПК-10 Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности;	современные средства криптографической и технической защиты информации	использовать и настраивать современные средства криптографической и технической защиты информации	навыками решения задач профессиональной деятельности с использованием современных средства криптографической и технической защиты информации
ОПК-11 Способен разрабатывать компоненты систем защиты информации автоматизированных систем;	структуру систем защиты информации автоматизированных систем.	выявлять основные компоненты системы защиты информации автоматизированных систем	навыками разработки компонентов систем защиты защиты информации автоматизированных систем
ОПК-12 Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем;	основные подходы к обеспечению безопасности вычислительных сетей, операционных систем и баз данных	настраивать компоненты и средства защиты информации для вычислительных сетей, операционных систем и баз данных	навыками обеспечения безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем
ОПК-13 Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем;	методы диагностики и тестирования систем защиты информации автоматизированных систем, методы анализа уязвимостей систем защиты информации автоматизированных систем	применять средства диагностики и тестирования систем защиты информации автоматизированных систем, средства анализа уязвимостей систем защиты информации автоматизированных систем	навыками диагностики и тестирования систем защиты информации автоматизированных систем, способен проводить анализ уязвимостей систем защиты информации автоматизированных систем
ОПК-14 Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений;	требования законодательства к защите информации в автоматизированных системах	проводить подготовку исходных данных для технико-экономического обоснования проектных решений для систем защиты информации в автоматизированных системах	навыками разработки, внедрения и эксплуатации автоматизированных систем в защищённом исполнении с учетом требований по защите информации
ОПК-15 Способен осуществлять администрирование и контроль	методы администрирования и контроля функционирования	применять средства администрирования и контроля функционирования	навыками администрирования и контроля функционирования

функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем;	средств и систем защиты информации автоматизированных систем, методы инструментального мониторинга защищенности автоматизированных систем	средств и систем защиты информации автоматизированных систем, применять средства инструментального мониторинга защищенности автоматизированных систем	средств и систем защиты информации автоматизированных систем, навыками инструментального мониторинга защищенности автоматизированных систем
ОПК-16 Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма.	основные закономерности исторического процесса; этапы исторического развития России, место и роль России в истории человечества и в современном мире; ключевые события истории России и мира с древности до наших дней, выдающихся деятелей отечественной истории; различные оценки и периодизации Отечественной истории	соотносить общие исторические процессы и отдельные факты, выявлять существенные черты исторических процессов, явлений и событий; извлекать уроки из исторических событий и на их основе принимать осознанные решения; осуществлять эффективный поиск информации и критику источников; получать, обрабатывать и сохранять источники информации; формулировать и аргументировано отстаивать собственную позицию по различным проблемам истории	представлениями о событиях российской и всемирной истории, основанными на принципе историзма; навыками анализа исторических источников; приёмами ведения дискуссии и полемики
ОПК-7.1. Способен использовать программные и программно-аппаратные средства для моделирования и испытания систем защиты информационных систем;	подходы к моделированию и испытанию систем защиты информации информационных систем	использовать программные и программно-аппаратные средства для моделирования систем защиты информационных систем	навыками использования программных и программно-аппаратных средства для моделирования и испытания систем защиты информационных систем
ОПК-7.2. Способен разрабатывать методики и тесты для анализа степени защищенности информационной системы и ее соответствия нормативным требованиям по защите информации;	нормативные требования по защите информации информационных систем	разрабатывать методики для анализа защищенности информационных систем	навыками разработки методики и тестов для анализа степени защищенности информационной системы и ее соответствия нормативным требованиям по защите информации
ОПК-7.3. Способен проводить анализ защищенности и верификацию программного обеспечения информационных систем;	методы анализа защищенности и верификации программного обеспечения	проводить анализ защищенности и верификацию программного обеспечения	навыками анализа защищенности и верификации программного обеспечения информационных систем
ПК-1 Обеспечение информационной	основные подходы к обеспечению	настраивать компьютерные системы	навыками обеспечения информационной

безопасности компьютерных систем и сетей	информационной безопасности компьютерных систем и сетей.	и сети в соответствии с требованиями по обеспечению информационной безопасности	безопасности компьютерных систем и сетей
ПК-2 Разработка систем защиты информации автоматизированных систем	основные требования нормативных документов в области защиты информации в автоматизированных системах; знает основные подходы к разработке систем защиты информации автоматизированных систем.	разрабатывать проекты систем защиты информации автоматизированных систем	навыками разработки систем защиты информации автоматизированных систем.
ПК-3 Формирование требований к защите информации в автоматизированных системах	требования законодательства к защите информации в автоматизированных системах; знает подходы к формированию требований по защите информации в автоматизированных системах	формировать требования к защите информации в автоматизированных системах на основании нормативных документов	навыками формирования требований к защите информации в автоматизированных системах на основании анализа и моделирования системы защиты информации
ПК-4 Организация и проведение работ по технической защите информации	основы организации работы коллектива и методы принятия управленческих решений	применять методы принятия управленческих решения для организации работы коллектива в профессиональной деятельности	навыками организации и проведения работ по технической защите информации для обеспечения информационной безопасности автоматизированных систем.
ПК-5 Проведение аттестации объектов на соответствие требованиям по защите информации	положения нормативных документов по аттестации объектов информатизации	проводить контроль защищенности автоматизированной системы от утечки по техническим каналам и от НСД к информации	навыками проведения аттестации автоматизированных систем на соответствие требованиям по защите информации

3.4.2. Критерии оценки результатов защиты выпускных квалификационных работ.

При выставлении оценки по результатам защиты выпускной квалификационной работы могут учитываться следующие требования:

1. Актуальность проблемы исследования:

- решение проблемы ориентировано на получение актуального знания;
- взаимообусловленность темы, цели, задач, объекта, предмета исследования,

2. Признаки научного исследования:

- наличие структурных элементов научного исследования,
- достаточность привлеченного теоретического и практического материала,
- современность использованного библиографического материала;

3. Концептуальность исследования:

- наличие теоретически обоснованной авторской позиции,

- обоснование выбора методов исследования (при наличии);

4. Практико-ориентированность исследования:

- практическая значимость проблемы исследования,

- практическая перспективность исследования;

5. Достоверность результатов исследования:

- использование обоснованного комплекса методов и методик сбора, анализа и интерпретации экспериментального материала (при наличии),

- достаточность экспериментальной выборки (при наличии);

6. Стиль, язык изложения, объем, оформление работы:

- изложение текста работы на профессиональном языке и в научном стиле;

- объем и оформление текста выпускной квалификационной работы в соответствии с установленными требованиями (раздел «Требования к выпускной квалификационной работе и порядку ее выполнения»).

Критерии оценивания результатов защиты выпускной квалификационной работы:

Критерии оценивания	
отлично	обучающийся способен самостоятельно искать, анализировать и оценивать профессиональную информацию; понимать методологические основы профессиональной деятельности; решать различные типы практических задач в профессиональной области, в том числе корректировать свои действия при изменении условий выполнения задачи, а также в различных рабочих ситуациях; осуществлять текущий и итоговый контроль своей, а при необходимости и групповой профессиональной деятельности, ее оценку и при необходимости коррекцию; принимать стратегические решения в сфере исполнения своих должностных обязанностей; проявлять полученные навыки при решении профессиональных задач различной сложности; избирать оригинальные пути решения сложных профессиональных задач. Оценка «отлично» ставится, если в процессе защиты подтверждается полное соответствие ВКР установленным и рекомендованным общим требованиям; обучающийся системно и последовательно излагает основное содержание исследования, демонстрирует полное и корректное толкование понятий и категорий; обнаруживает понимание материала работы, может обосновать свои суждения, выводы и предложения, их применение на практике – со ссылкой на источники; содержательно и аргументированно отвечает на все поставленные вопросы.
хорошо	обучающийся способен самостоятельно искать, анализировать и оценивать профессиональную информацию; способен решать различные типы практических задач в профессиональной области, в том числе корректировать свои действия при изменении условий выполнения задачи, а также в различных рабочих ситуациях; осуществлять текущий и итоговый контроль своей профессиональной деятельности, ее оценку и при необходимости коррекцию; владеет сложными навыками в сфере своей профессиональной деятельности, способен, используя их, активно влиять на происходящее, самостоятельно принимать решения в сфере профессиональной деятельности и проявлять полученные навыки в ситуациях различной сложности. Оценка «хорошо» ставится, если в процессе защиты подтверждается полное соответствие ВКР установленным и рекомендованным общим требованиям; обучающийся последовательно излагает основное содержание исследования, демонстрирует корректное толкование понятий и категорий; обнаруживает понимание материала, может обосновать свои суждения, выводы и

	предложения, их применение на практике, аргументированно отвечает на все поставленные вопросы, но допускает 1-2 ошибки, которые сам же исправляет, и (или) 1-2 недочета в последовательности и содержательно оформлении излагаемого.
удовлетворительно	обучающийся имеет представление о том, какие именно способности должны сформироваться в процессе обучения по данному направлению; способен самостоятельно искать, анализировать и использовать профессиональную информацию; способен, используя полученные знания и навыки, самостоятельно на должном уровне осуществлять основные виды профессиональной деятельности, решать различные типы практических задач в профессиональной области, в том числе корректировать свои действия при изменении условий выполнения задачи, самостоятельно контролировать, оценивать и корректировать свою профессиональную деятельность. Оценка «удовлетворительно» ставится, если в процессе защиты в целом подтверждается соответствие ВКР установленным и рекомендованным общим требованиям; обучающийся обнаруживает знание и понимание основных положений тематики исследования, но излагает материал неполно и допускает неточности в определении понятий или формулировке норм и правил; не умеет достаточно глубоко и доказательно обосновать свои суждения, выводы, предложения или привести примеры; излагает материал непоследовательно и допускает ошибки; отвечает частично на поставленные вопросы.
неудовлетворительно	обучающийся не владеет необходимыми для осуществления профессиональной деятельности знаниями и навыками, или владеет ими фрагментарно, не способен их применять в процессе профессиональной деятельности, не способен решать типовые профессиональные задачи. Оценка «неудовлетворительно» ставится, если в процессе защиты частично подтверждается соответствие ВКР установленным и рекомендованным общим требованиям; обучающийся обнаруживает незнание большей части материала исследования; допускает ошибки в формулировке определений и правил, искажающие их смысл; беспорядочно и неуверенно излагает содержание работы; отвечает частично или отказывается от ответа на поставленные вопросы, уровень самостоятельности выполнения работы составляет: менее 50% по программам бакалавриата и специалитета, менее 60 % - по программам магистратуры (с учетом заключения о проведении проверки ВКР на предмет объема заимствований с использованием системы «Антиплагиат»).

3.5. Методические материалы по защите выпускной квалификационной работы

3.5.1. Требования к выпускной квалификационной работе и порядку ее выполнения:

Общие требования к выпускной квалификационной работе содержат общие положения, цели и задачи выпускной квалификационной работы, требования к тексту и оформлению выпускной квалификационной работы. Требования размещены:

https://www.syktsu.ru/sveden/education/Требования%20к%20ВКР.pdf

ВКР представляет собой теоретическое и/или экспериментальное исследование одной из актуальных проблем по информационной безопасности, при её выполнении студент должен показать свою способность и умение, опираясь на полученные знания, решать на современном уровне научные и научно-практические задачи, грамотно излагать специальную информацию, докладывать и отстаивать свою точку зрения перед аудиторией.

ВКР представляют собой:

- самостоятельное научное исследование;

- работу прикладного характера;

- работу методического характера.

Выпускные квалификационные работы могут выполняться по открытым или закрытым темам (работы с грифом). Порядок защиты закрытых работ определяется отдельным нормативным актом.

3.5.2. Методические рекомендации по подготовке выпускных квалификационных работ.

Методические рекомендации по подготовке выпускных квалификационных работ, содержат информацию об основных этапах исследования, рекомендации по работе над рукописью, требования к оформлению работы и размещены:

https://www.syktsu.ru/sveden/education/Методические рекомендации КР и ВКР.pdf

4. Порядок подачи и рассмотрения апелляций

Порядок подачи и рассмотрения апелляций определен в Положении об итоговой (государственной итоговой) аттестации по образовательным программам высшего образования - программам бакалавриата, программам специалитета и программам магистратуры.

5. Материально техническое обеспечение итоговой (государственной итоговой) аттестации

Университет на законном основании располагает материально-техническим базой (помещениями и оборудованием) для проведения итоговой (государственной итоговой) аттестация по основной профессиональной образовательной программе в соответствии с учебным планом.

Сведения о материально-техническом обеспечении итоговой (государственной итоговой) аттестация содержатся в справке о материально-технических условиях реализации образовательной программы.

6. Особенности проведения итоговой (государственной итоговой) аттестации для обучающихся с ограниченными возможностями здоровья и инвалидов

Проведение итоговой (государственной итоговой) аттестации для обучающихся с ограниченными возможностями здоровья и инвалидов осуществляется в соответствии с законодательством Российской Федерации.

Для обучающихся из числа инвалидов итоговая (государственная итоговая) аттестация проводится университетом с учетом особенностей их психофизического развития, индивидуальных возможностей и состояния здоровья.

Программа итоговой (государственной итоговой) аттестации и другие локальные акты университета по вопросам проведения итоговой (государственной итоговой) аттестации доводятся до сведения обучающихся инвалидов в доступной для них форме.