

МИНОБРНАУКИ РОССИИ



Федеральное государственное бюджетное образовательное учреждение
высшего образования

«Российский государственный гуманитарный университет»

(ФГБОУ ВО «РГГУ»)

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ

Кафедра комплексной защиты информации



УТВЕРЖДАЮ

Первый проректор-

проректор по научной работе

О.В. Павленко

**МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ,
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**

ПРОГРАММА ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

Направление подготовки 10.06.01 Информационная безопасность

Направленность программ подготовки научно-педагогических кадров в
аспирантуре:

«Методы и системы защиты информации, информационная безопасность»

Москва 2019

Методы и системы защиты информации, информационная безопасность
ПРОГРАММА ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ
Направление подготовки 10.06.01 Информационная безопасность
Направленность программы подготовки научно-педагогических кадров в аспирантуре
«Методы и системы защиты информации, информационная безопасность»

Составитель: Д.А. Митюшин,
кандидат технических наук

Программа утверждена
на заседании кафедры комплексной защиты информации
30 августа 2019 г., протокол № 1

Программа утверждена
на заседании Совета института
30 августа 2019 г., протокол № 1

Программа утверждена
на заседании Научно-методического совета
по аспирантуре и докторантуре
28 ноября 2019 г., протокол № 1

1. Пояснительная записка

Государственная итоговая аттестация обучающихся по программам подготовки научно-педагогических кадров в аспирантуре проводится в форме:

государственного экзамена;

представления научного доклада об основных результатах подготовленной научно-квалификационной работы (далее – научный доклад; вместе – государственные аттестационные испытания).

Программа государственной итоговой аттестации состоит из двух частей. В первой определены цель и задачи итогового государственного экзамена, требования к нему, представлены содержание и порядок прохождения итогового государственного экзамена. Во второй сформулированы требования к научному докладу об основных результатах подготовленной научно-квалификационной работы.

Государственный экзамен является частью итоговой аттестации аспиранта. Его цель – выявить теоретическую подготовку аспиранта к решению научных задач и преподаванию дисциплин, соответствующих направлению подготовки 10.06.01 – Информационная безопасность (направленность программы подготовки научно-педагогических кадров в аспирантуре: «Методы и системы защиты информации, информационная безопасность»).

Государственный экзамен проводится государственными экзаменационными комиссиями в целях определения соответствия результатов освоения обучающимися образовательных программ требованиям соответствующего образовательного стандарта.

Данная программа составлена на основании программ курсов, преподаваемых в аспирантуре в Институте информационных наук и технологий безопасности РГГУ в соответствии с учебным планом. К итоговому государственному экзамену допускаются выпускники, завершившие полный курс обучения, успешно прошедшие предшествующие испытания, предусмотренные учебным планом.

Государственный экзамен включает вопросы, результаты освоения которых имеют значение для профессиональной деятельности выпускников, в том числе для преподавательского и научного видов деятельности. На экзамен выносятся вопросы по дисциплинам «Информатизация общества и информационная безопасность», «Защита информации от несанкционированного воздействия. Современные проблемы информационно-измерительного обеспечения», «Методы и системы инженерно-технической защиты информации», «Методология и методы исследования систем защиты информации, информационной безопасности».

Экзамен проводится устно.

В ходе государственных аттестационных испытаний проверяются следующие **компетенции выпускника аспирантуры:**

универсальные (УК):

способность к критическому анализу и оценке современных научных достижений, генерированию новых идей при решении исследовательских и практических задач, в том числе в междисциплинарных областях (УК-1),

способность проектировать и осуществлять комплексные исследования, в том числе междисциплинарные, на основе целостного системного научного мировоззрения с использованием знаний в области истории и философии науки (УК-2),

готовность участвовать в работе российских и международных исследовательских коллективов по решению научных и научно-образовательных задач (УК-3),

готовностью использовать современные методы и технологии научной коммуникации на государственном и иностранном языках (УК-4),

способность следовать этическим нормам в профессиональной деятельности (УК-5),

способность планировать и решать задачи собственного профессионального и личностного развития (УК-6),

общефессиональные (ОПК):

способность формулировать научные задачи в области обеспечения информационной безопасности, применять для их решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность (ОПК-1);

способность разрабатывать частные методы исследования и применять их в самостоятельной научно-исследовательской деятельности для решения конкретных исследовательских задач в области обеспечения информационной безопасности (ОПК-2),

способность обоснованно оценивать степень соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности (ОПК-3);

способностью организовать работу коллектива по проведению научных исследований в области информационной безопасности (ОПК-4);

готовностью к преподавательской деятельности по основным образовательным программам высшего образования (ОПК-5);

профессиональные (ПК) для направленности «Сравнительно-историческое, типологическое и сопоставительное языкознание»:

способность самостоятельно осуществлять научно-исследовательскую деятельность в сфере защиты информации, используя современные научный инструментарий и информационно-коммуникативные практики, принимая во внимание специфику объектов обеспечения информационной безопасности во всех сферах деятельности (ПК-1);

готовность к образовательной деятельности по направлению «информационная безопасность» в рамках направленности «методы и системы защиты информации, информационная безопасность», в том числе с использованием современных мультимедийных и сетевых технологий (ПК-2).

Аспирант должен:

знать:

нормативно-методическую базу в области информационной безопасности, факторы, определяющие её развитие, механизмы влияния на неё со стороны государства, знать методы, модели и средства выявления, идентификации и классификации угроз нарушения информационной безопасности (УК-1, ОПК-1, ОПК-3, ОПК-4, ОПК-5, ПК-1, ПК-2);

меры по обеспечению сохранности информации, основные задачи обеспечения безопасности информации в информационных системах; принципы построения систем защиты информации и их основы; основные направления создания защищенных информационных систем, определения и свойства математических объектов, используемых в этой области (ОПК-1, ОПК-3, ПК-1);

методы анализа и оценки современных научных достижений в области информационной безопасности, а также принципы генерирования новых идей при решении исследовательских и практических задач, в том числе в междисциплинарных областях (УК-1, УК-2, ОПК-1, ОПК-3, ПК-1);

методы научно-исследовательской деятельности (УК-2, ОПК-1, ОПК-3, ПК-1);

особенности представления результатов научной деятельности в устной и письменной форме при работе в российских и международных исследовательских коллективах (УК-3, УК-5, УК-6, ОПК-1, ОПК-3, ПК-1);

методику и технологии научной коммуникации на государственном и иностранном языках (УК-3, УК-5, УК-6);

уметь:

анализировать источники и литературу в области информационной безопасности, соотносить этот анализ с политической стратегией развития России в области информационной безопасности; определять модели противодействия угрозам нарушения информационной безопасности для любого вида информационных систем (УК-1, ОПК-1, ОПК-3);

участвовать в дискуссиях, а также в выработке коллективных решений (УК-1, УК-3, УК-5, ОПК-1, ОПК-3);

анализировать альтернативные варианты решения исследовательских и практических задач и оценивать потенциальные возможности реализации этих вариантов (УК-1, УК-6, ОПК-3, ПК-1);

следовать нормам научного общения при работе в российских и международных исследовательских коллективах с целью решения научных и научно-образовательных задач (УК-3, УК-5, ОПК-3);

владеть:

математическим аппаратом, используемым в системах защиты информации, основными алгоритмами, классификацией способов защиты информации; методами защиты информации от несанкционированного доступа и разрушающих программных воздействий процесса хранения и обработки информации (УК-1, УК-2, ОПК-1, ОПК-3, ПК-1);

методиками и технологиями планирования профессиональной деятельности в сфере научных исследований (УК-3, УК-6, ОПК-1, ОПК-3, ПК-1);

методиками и технологиями планирования коллективной деятельности по решению научных задач (УК-3, ОПК-3);

методиками и технологиями оценки результатов коллективной деятельности по решению научных задач (УК-3, ОПК-3);

различными типами коммуникаций при осуществлении организационной и научной работы в коллективе (УК-3, ОПК-3);

навыками применения полученных знаний в научно-педагогической работе (УК-1, УК-2, ОПК-1, ОПК-3, ПК-1).

Процедура государственных аттестационных испытаний.

Экзамен проводится в устной форме. Государственный экзамен включает вопросы, результаты освоения которых имеют значение для профессиональной деятельности выпускников, в том числе для преподавательского и научного видов деятельности. В перечень вопросов, задаваемых в ходе государственного экзамена, включается вопрос о разработанных аспирантом в ходе педагогической практики учебно-методических материалах.

Экзаменационный билет содержит три вопроса.

Максимальное время на подготовку к ответу – 20 минут.

В зависимости от индивидуальных особенностей обучающихся с ограниченными возможностями здоровья РГГУ обеспечивает выполнение следующих требований при проведении государственного аттестационного испытания:

а) для слепых:

задания и иные материалы для сдачи государственного аттестационного испытания оформляются рельефно-точечным шрифтом Брайля или в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением для слепых, либо зачитываются ассистентом;

письменные задания выполняются обучающимися на бумаге рельефно-точечным шрифтом Брайля или на компьютере со специализированным программным обеспечением для слепых, либо надиктовываются ассистенту;

при необходимости обучающимся предоставляется комплект письменных принадлежностей и бумага для письма рельефно-точечным шрифтом Брайля, компьютер со специализированным программным обеспечением для слепых;

б) для слабовидящих:

задания и иные материалы для сдачи государственного аттестационного испытания оформляются увеличенным шрифтом;

обеспечивается индивидуальное равномерное освещение не менее 300 люкс;

при необходимости обучающимся предоставляется увеличивающее устройство, допускается использование увеличивающих устройств, имеющихся у обучающихся;

в) для глухих и слабослышащих, с тяжелыми нарушениями речи:

обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости обучающимся предоставляется звукоусиливающая аппаратура индивидуального пользования;

по их желанию государственные аттестационные испытания проводятся в письменной форме.

В ходе экзамена не допускается использование конспектов, справочной, профессиональной и учебной литературы; электронных средств (мобильных телефонов, карманных компьютеров-коммуникаторов, ноутбуков, цифровых фотоаппаратов и так далее). В случае нарушения указанных правил аспирант удаляется с экзамена и получает оценку «неудовлетворительно».

Члены Государственной экзаменационной комиссии имеют право задавать студентам дополнительные вопросы в рамках вопросов билета.

По окончании ответов аспирантов члены Государственной экзаменационной комиссии совещаются, обсуждая каждый ответ аспирантов. По итогам обсуждения выставляется оценка: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Критерии оценки результатов государственных аттестационных испытаний

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

Оценка «отлично» выставляется, если аспирант показывает глубокие знания всего программного материала, даёт последовательные, содержательные, полные, правильные и конкретные ответы на все вопросы экзаменационного билета, а также на дополнительные вопросы экзаменаторов.

Оценка «хорошо» ставится аспиранту, если он демонстрирует знание программного материала, но вопросы экзаменационного билета раскрывает недостаточно глубоко и не даёт полных ответов на дополнительные вопросы.

Оценка «удовлетворительно» выставляется, если аспирант отвечает на вопросы экзаменационного билета, допуская негрубые ошибки, неточности, а также недостаточно ориентируется в освещаемом материале при ответе как на основные, так и на дополнительные вопросы.

Оценка «неудовлетворительно» ставится аспиранту, который даёт неправильный ответ на один из вопросов экзаменационного билета, допускает грубые ошибки, проявляет непонимание сути излагаемых вопросов.

Критерии оценки результатов представления научного доклада

При итоговой оценке учитываются следующие показатели:

- актуальность исследования,
- наличие новых результатов и положений (научная новизна),
- аргументированность выводов, их соответствие заявленным целям и задачам,
- практическая (теоретическая) значимость работы,
- методологическая чёткость и достоверность полученных результатов,
- наличие публикаций в российских и зарубежных рецензируемых изданиях, в том числе в журналах из перечня ВАК,
- качество выполнения презентации,
- отзыв научного руководителя и рецензента работы.

Успешное прохождение государственной итоговой аттестации является основанием для выдачи обучающемуся документа о высшем образовании и о квалификации образца,

установленного Минобрнауки России, по программам подготовки научно-педагогических кадров в аспирантуре.

Выпускникам, успешно освоившим образовательную программу подготовки научно-педагогических кадров в аспирантуре, выдаётся заключение в соответствии с пунктом 16 Положения о присуждении учёных степеней, утверждённого постановлением Правительства Российской Федерации от 24 сентября 2013 г. № 842.

2. ПЕРЕЧЕНЬ ВОПРОСОВ К ГОСУДАРСТВЕННОМУ ЭКЗАМЕНУ

1. Информатизация общества и информационная безопасность

№ пп	Перечень вопросов к государственному экзамену	Проверяемые компетенции
1.	Архитектура построения безопасности систем коммуникаций компьютерных систем из стандарта ГОСТ Р ИСО 7498, часть 2.	УК-1 – УК-6, ОПК-1 – ОПК-5, ПК-1, ПК-2
2.	Классификация угроз нарушения информационной безопасности.	УК-1 – УК-6, ОПК-1 – ОПК-5, ПК-1, ПК-2
3.	Каковы уязвимости современных программно-аппаратных систем.	УК-1 – УК-6, ОПК-1 – ОПК-5, ПК-1, ПК-2
4.	Продукты, реализующие электронный документооборот.	УК-1 – УК-6, ОПК-1 – ОПК-5, ПК-1, ПК-2
5.	Межсетевые экраны и их характеристики.	УК-1 – УК-6, ОПК-1 – ОПК-5, ПК-1, ПК-2
6.	Профили защиты для межсетевых экранов.	УК-1 – УК-6, ОПК-1 – ОПК-5, ПК-1, ПК-2
7.	Продукты защиты на отечественном рынке.	УК-1 – УК-6, ОПК-1 – ОПК-5, ПК-1, ПК-2
8.	Модели скрытых каналов	УК-1 – УК-6, ОПК-1 – ОПК-5, ПК-1, ПК-2
9.	Вероятностные оценки сбоев и стихийных бедствий.	УК-1 – УК-6, ОПК-1 – ОПК-5, ПК-1, ПК-2
10.	Оценки надёжности систем телекоммуникаций и протоколов связи.	УК-1 – УК-6, ОПК-1 – ОПК-5, ПК-1, ПК-2
11.	Процедуры сертификации и аттестации и их реализация.	УК-1 – УК-6, ОПК-1 – ОПК-5, ПК-1, ПК-2
12.	Методы анализа аудита. Системы мониторинга больших информационных систем.	УК-1 – УК-6, ОПК-1 – ОПК-5, ПК-1, ПК-2
13.	Процедура обследования объектов информатизации.	УК-1 – УК-6, ОПК-1 – ОПК-5, ПК-1, ПК-2
14.	Экспертная оценка защищённости и уровня доверия.	УК-1 – УК-6, ОПК-1 – ОПК-5, ПК-1, ПК-2
15.	Системы обнаружения вторжений и формирование безопасной среды с помощью «событий безопасности».	УК-1 – УК-6, ОПК-1 – ОПК-5, ПК-1, ПК-2
16.	Процедуры досертификации и перееаттестации.	УК-1 – УК-6, ОПК-1 – ОПК-5, ПК-1, ПК-2
17.	Безопасное администрирование	УК-1 – УК-6, ОПК-1 – ОПК-5, ПК-1, ПК-2

2. Защита информации от несанкционированного воздействия. Современные проблемы информационно-измерительного обеспечения

№ пп	Перечень вопросов к государственному экзамену	Проверяемые компетенции
1.	Математические модели сложных сигналов и их физическая интерпретация.	УК-1 – УК-6, ОПК-1 – ОПК-5, ПК-1, ПК-2
2.	Описание физических процессов в трёхмерном пространстве.	УК-1 – УК-6, ОПК-1 – ОПК-5, ПК-1, ПК-2

3.	Вычислительные процедуры спектрального представления сигналов.	УК-1 – УК-6, ОПК-1 – ОПК-5, ПК-1, ПК-2
4.	Проблемы оценки нелинейных корреляционных связей.	УК-1 – УК-6, ОПК-1 – ОПК-5, ПК-1, ПК-2
5.	Современные методы наблюдения и измерения сигнала.	УК-1 – УК-6, ОПК-1 – ОПК-5, ПК-1, ПК-2
6.	Взаимодействие сигнала с детерминированными и случайными помехами при регистрации во временной области.	УК-1 – УК-6, ОПК-1 – ОПК-5, ПК-1, ПК-2
7.	Особенности спектральных характеристик сигнала, получаемых при БПФ записи отрезка временной зависимости	УК-1 – УК-6, ОПК-1 – ОПК-5, ПК-1, ПК-2
8.	Многоканальные и компенсационные измерительные системы в трёхмерном пространстве.	УК-1 – УК-6, ОПК-1 – ОПК-5, ПК-1, ПК-2
9.	Особенности сигналов, формируемых современной аппаратурой обработки и защиты информации.	УК-1 – УК-6, ОПК-1 – ОПК-5, ПК-1, ПК-2
10.	Перспективные направления анализа широкополосного излучения.	УК-1 – УК-6, ОПК-1 – ОПК-5, ПК-1, ПК-2
11.	Генераторы шума на основе цифровых генераторов псевдослучайных последовательностей.	УК-1 – УК-6, ОПК-1 – ОПК-5, ПК-1, ПК-2
12.	Построение генераторов шума на основе случайных процессов в микромире	УК-1 – УК-6, ОПК-1 – ОПК-5, ПК-1, ПК-2

3. Методы и системы инженерно-технической защиты информации

№ пп	Перечень вопросов к государственному экзамену	Проверяемые компетенции
1.	Функциональные особенности объектов защиты	УК-1 – УК-6, ОПК-1 – ОПК-5, ПК-1, ПК-2
2.	Локальные особенности объектов защиты	УК-1 – УК-6, ОПК-1 – ОПК-5, ПК-1, ПК-2
3.	Демаскирующие признаки объектов защиты.	УК-1 – УК-6, ОПК-1 – ОПК-5, ПК-1, ПК-2
4.	Защита объекта информатизации от видового наблюдения.	УК-1 – УК-6, ОПК-1 – ОПК-5, ПК-1, ПК-2
5.	Утечка информации за счёт побочных электромагнитных полей и наводок.	УК-1 – УК-6, ОПК-1 – ОПК-5, ПК-1, ПК-2
6.	Утечка информации за счёт функциональных излучений и по каналам связи.	УК-1 – УК-6, ОПК-1 – ОПК-5, ПК-1, ПК-2
7.	Акустические каналы утечки информации	УК-1 – УК-6, ОПК-1 – ОПК-5, ПК-1, ПК-2
8.	Защита от утечки информации за счёт внедрения ретрансляторов и зондирования направленным излучением.	УК-1 – УК-6, ОПК-1 – ОПК-5, ПК-1, ПК-2
9.	Системы охраны объекта и управления доступом как фактор информационной безопасности.	УК-1 – УК-6, ОПК-1 – ОПК-5, ПК-1, ПК-2
10.	Виды контроля защищённости объекта.	УК-1 – УК-6, ОПК-1 – ОПК-5, ПК-1, ПК-2
11.	Аттестация объектов информатизации.	УК-1 – УК-6, ОПК-1 – ОПК-5, ПК-1, ПК-2

4. Методология и методы исследования систем защиты информации, информационной безопасности

№ пп	Перечень вопросов к государственному экзамену	Проверяемые компетенции
1.	Системный подход в построении систем защиты информации и в обеспечении информационной безопасности.	УК-1 – УК-6, ОПК-1 – ОПК-5, ПК-1, ПК-2
2.	Модель построения системы информационной безопасности организации.	УК-1 – УК-6, ОПК-1 – ОПК-5, ПК-1, ПК-2
3.	Основные принципы защиты информации.	УК-1 – УК-6, ОПК-1 – ОПК-5, ПК-1, ПК-2
4.	Разработка концепции обеспечения ИБ.	УК-1 – УК-6, ОПК-1 – ОПК-5, ПК-1, ПК-2
5.	Понятие эффективности. Показатели и критерии эффективности. Отношение «эффективность/стоимость».	УК-1 – УК-6, ОПК-1 – ОПК-5, ПК-1, ПК-2
6.	Эффективность комплексной системы защиты информации и обеспечения информационной безопасности	УК-1 – УК-6, ОПК-1 – ОПК-5, ПК-1, ПК-2
7.	Модели систем обнаружения вторжений. Классификация систем обнаружения вторжений.	УК-1 – УК-6, ОПК-1 – ОПК-5, ПК-1, ПК-2
8.	Система обнаружения вторжений Snort. Правила Snort. Примеры правил.	УК-1 – УК-6, ОПК-1 – ОПК-5, ПК-1, ПК-2
9.	Обнаружение аномалий. Методы Data Mining.	УК-1 – УК-6, ОПК-1 – ОПК-5, ПК-1, ПК-2
10.	Системы анализа защищённости. Системы анализа целостности. Вспомогательные средства обнаружения.	УК-1 – УК-6, ОПК-1 – ОПК-5, ПК-1, ПК-2
11.	Методы обхода сетевых и хостовых систем обнаружения вторжений.	УК-1 – УК-6, ОПК-1 – ОПК-5, ПК-1, ПК-2
12.	Системы предупреждения вторжений.	УК-1 – УК-6, ОПК-1 – ОПК-5, ПК-1, ПК-2
13.	Аудит безопасности информации предприятия и методы его проведения	УК-1 – УК-6, ОПК-1 – ОПК-5, ПК-1, ПК-2

Литература к вопросам государственного экзамена

1. Указ Президента РФ от 05.12.2016 № 646 "Об утверждении Доктрины информационной безопасности Российской Федерации" [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_208191/, свободный. – Загл. с экрана.
2. Указ Президента РФ от 06.03.1997 № 188 (ред. от 13.07.2015) «Об утверждении Перечня сведений конфиденциального характера» [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_13532/, свободный. – Загл. с экрана.
3. Указ Президента РФ от 09.05.2017 № 203 "О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы" [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_216363/, свободный. – Загл. с экрана.
4. Указ Президента РФ от 30.11.1995 № 1203 (ред. от 08.08.2019) «Об утверждении

- Перечня сведений, отнесённых к государственной тайне» [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_8522/, свободный. – Загл. с экрана.
5. Указ Президента РФ от 31.12.2015 № 683 "О Стратегии национальной безопасности Российской Федерации" [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_191669/, свободный. – Загл. с экрана.
 6. Федеральный закон "О персональных данных" от 27.07.2006 № 152-ФЗ (последняя редакция). [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_61801/, свободный. – Загл. с экрана.
 7. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (последняя редакция). [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_61798/, свободный. – Загл. с экрана.
 8. Федеральный закон РФ от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_48699/, свободный. – Загл. с экрана.
 9. ГОСТ Р 54989-2012 / ISOTR18492:2005. Обеспечение долговременной сохранности электронных документов" [Электронный ресурс] : Режим доступа : <http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=OTN&n=2489#0005936991809006864>, свободный. – Загл. с экрана.
 10. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности требования [Электронный ресурс] : Режим доступа : <http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=OTN&n=9032#011028370269284904>, свободный. – Загл. с экрана.
 11. ГОСТ Р ИСО/МЭК 27004-2011. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения" [Электронный ресурс] : Режим доступа : <http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=OTN&n=388#041622976189257066>, свободный. – Загл. с экрана.
 12. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. [Электронный ресурс] : Режим доступа : <http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=OTN&n=666#05511035764404268>, свободный. – Загл. с экрана.
 13. Баранова, Е. К. Информационная безопасность и защита информации : учеб. пособие / Баранова Е.К., Бабаш А.В. – 4-е изд., перераб. и доп. – Москва : РИОР : ИНФРА-М, 2019. – 322 с. – (Высшее образование). – www.dx.doi.org/10.12737/11380. - ISBN 978-5-16-106532-7. – Текст : электронный. – URL: <https://new.znaniium.com/catalog/product/1009606> (дата обращения: 25.08.2019)
 14. Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика».
 15. Грекул, В. И. Аудит информационных технологий: Учебник для вузов / Грекул В.И. - Москва :Гор. линия-Телеком, 2015. - 154 с. (Специальность) ISBN 978-5-9912-0528-3. - Текст : электронный. - URL: <https://new.znaniium.com/catalog/product/555524> (дата обращения: 25.08.2019)
 16. Грушо А.А. Теоретические основы компьютерной безопасности. – М.: Изд. Центр «Академия», 2009. - 272 с.
 17. Зайцев, А. П. Технические средства и методы защиты информации: Учебник для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В.Мещеряков; Под ред. А.П.Зайцева - 7 изд., исправ. - Москва : Гор. линия-Телеком, 2012. - 442с.; - (Уч. для вузов). ISBN 978-5-9912-0233-6. - Текст : электронный. - URL: <https://new.znaniium.com/catalog/product/390284> (дата обращения: 25.08.2019)

18. Закон РФ «О государственной тайне» от 21.07.1993 № 5485-1 (последняя редакция) [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_2481/, свободный. – Загл. с экрана.
19. Инженерно-техническая защита информации : учеб. пособие для студентов вузов, обучающихся по специальностям в обл. информ. безопасности / А. А. Торокин. - М. : Гелиос АРВ, 2005. - 958 с. : рис.,табл. - Библиогр.: с. 934-949. - ISBN 5-85438-140-0. - ISBN 5-85438-140-0(ошибоч.) : 275.
20. Коваленко Ю.И. Правовой режим лицензирования и сертификации в сфере информационной безопасности : учеб. пособие для слушателей, обучающихся по программе доп. проф. образования в области информ. безопасности "Основы лицензирования и сертификации в области защиты информации" / Ю. И. Коваленко. - Москва : Горячая линия-Телеком, 2012. - 138 с. : табл. ; 21 см. - (Учебное пособие для высших учебных заведений). - Библиогр.: с. 134-138. - ISBN 978-5-9912-0261-9 : 341.00.
21. Конституция Российской Федерации от 25 декабря 1993 года, с изменениями от 30 декабря 2008 года (последняя редакция). [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_28399/, свободный. – Загл. с экрана.
22. Малюк, А. А. Защита информации в информационном обществе: Учебное пособие для вузов / Малюк А.А. - Москва : Гор. линия-Телеком, 2015. - 230 с. ISBN 978-5-9912-0481-1. - Текст : электронный. - URL: <https://new.znanium.com/catalog/product/536930> (дата обращения: 18.08.2019).
23. Обеспечение информационной безопасности бизнеса / Андрианов В.В., Зефиров С.Л., Голованов В.Б. - Москва :ЦИПСИР, 2011. - 373 с. ISBN 978-5-9614-1364-9 - Текст : электронный. - URL: <https://new.znanium.com/catalog/product/556539> (дата обращения: 18.08.2019)
24. Шелухин, О. И. Обнаружение вторжений в компьютерные сети (сетевые аномалии): Учебное пособие для вузов / О.И. Шелухин, Д.Ж. Сакалема, А.С. Филинова. - Москва : Гор. линия-Телеком, 2013. - 220 с.: ил.; . ISBN 978-5-9912-0323-4, 500 экз. - Текст : электронный. - URL: <https://new.znanium.com/catalog/product/421968> (дата обращения: 25.12.2019)

НАУЧНЫЙ ДОКЛАД

Представление научного доклада об основных результатах подготовленной научно-квалификационной работы (диссертации) (далее – доклад) является обязательной формой государственной итоговой аттестации и выполняется согласно графику учебного процесса.

Доклад имеет своей целью отразить личное участие обучающегося в получении результатов, изложенных в научно-квалификационной работе (диссертации).

Представление основных результатов выполненной научно-квалификационной работы по теме, утверждённой кафедрой, в рамках направленности образовательной программы, проводится в форме научного доклада.

После завершения подготовки обучающимся научно-квалификационной работы его научный руководитель даёт письменный отзыв о выполненной научно-квалификационной работе обучающегося (далее – отзыв).

Научно-квалификационные работы подлежат внутреннему и внешнему рецензированию. Рецензенты в сроки, установленные кафедрой, проводят анализ и представляют в организацию письменные рецензии на указанную работу (далее – рецензия).

Для проведения внутреннего рецензирования научно-квалификационной работы кафедрой назначаются один рецензент из числа научно-педагогических работников кафедры, имеющих научные труды по научной специальности (научным специальностям), соответствующей теме научно-квалификационной работы.

Кафедра обеспечивает проведение внешнего рецензирования научно-квалификационной работы.

Кафедра обеспечивает ознакомление обучающегося с отзывом и рецензией (рецензиями) не позднее чем за 7 календарных дней до представления научного доклада об основных результатах подготовленной научно-квалификационной работы.

Перед представлением научного доклада об основных результатах научно-квалификационной работы в сроки, установленные кафедрой, указанная работа, отзыв научного руководителя и рецензии передаются в государственную экзаменационную комиссию.

Требования к научному докладу

В рамках представления доклада оценивается степень соответствия практической и теоретической подготовленности выпускника к выполнению профессиональных задач, степени освоения компетенций, установленных ФГОС ВО. Подготовленная научно-квалификационная работа должна соответствовать критериям, установленным для научно-квалификационной работы (диссертации) на соискание учёной степени кандидата наук, и оформлена в соответствии с требованиями, устанавливаемыми Минобрнауки России.

Тексты научных докладов¹ размещаются в электронно-библиотечной системе университета.

В научном докладе излагаются основные идеи и выводы диссертации, показывается вклад автора в проведённое исследование, степень новизны и практическая значимость приведённых результатов исследований, содержатся сведения об организации, в которой выполнялась диссертация, о научных руководителях, приводится список публикаций автора диссертации, в которых отражены основные научные результаты диссертации. Объем научного доклада составляет от 1 до 1,5 авторского листа.

Тексты научно-квалификационной работы и научных докладов проверяются на объем заимствования.

В целях установления степени оригинальности текста научного доклада в РГГУ применяется система «Антиплагиат. ВУЗ».

Оригинальный текст научно-квалификационной работы и научного доклада об основных результатах подготовленной научно-квалификационной работы (диссертации) должен составлять 80 и более процентов общего объёма текста.

Требования к представлению доклада

Для доклада основных положений подготовленной научно-квалификационной работы, обоснования сделанных им выводов и предложений аспиранту предоставляется 15 минут, что соответствует 5–5,5 страницам обычного текста размером шрифта – 14, набранного с полуторным (1,5) межстрочным интервалом.

Доклад следует начинать с обоснования актуальности темы исследования, его целей и задач, далее по главам раскрывается основное содержание квалификационной работы, а затем освещаются основные результаты работы, сделанные выводы и предложения. Аспирант должен сделать свой доклад свободно, не читая письменного текста. Текст выступления должен быть максимально приближен к тексту квалификационной работы, поэтому основу выступления составляют введение и заключение, которые используются в выступлении практически полностью.

Рекомендуется в процессе доклада использовать заранее подготовленный наглядный графический (таблицы, схемы) или иной материал иллюстрирующий основные положения работы.

В ходе доклада должны быть использованы только те графики, диаграммы и схемы, которые приведены в диссертации. Использование в выступлении данных, не использованных в квалификационной работе, недопустимо.

¹ Научный доклад оформляется с учётом требований к автореферату диссертации на соискание учёной степени кандидата наук, изложенных в п. 25 постановления Правительства Российской Федерации от 24.09.2013 N 842 "О порядке присуждения учёных степеней".

Защита научного доклада

Процедура защиты научного доклада включает:

- представление аспиранта (называются фамилии, имя, отчество, тема, научный руководитель);
- доклад о поставленных целях и задачах, полученных результатах и выводах, их теоретической и практической значимости (10-15 мин);
- оглашение отзыва руководителя и рецензии;
- ответы аспиранта на сделанные замечания;
- вопросы членов ГЭК и присутствующих на защите к выпускнику;
- обмен мнениями о работе, в котором могут принять участие члены ГЭК, руководитель, консультант, рецензент и все желающие (слово присутствующим предоставляет председатель ГЭК);
- заключительное слово автора работы, в котором он может разъяснить положения, вызвавшие неясность или возражения, дать необходимые справки, привести дополнительные аргументы, поблагодарить руководителя, преподавателей и рецензентов за помощь в работе.

После окончания защиты доклада члены ГЭК обсуждают результаты защиты научного доклада, оценивают его с учётом качества подготовленной работы и процесса доклада. Обсуждение результатов защиты проводится на закрытом заседании ГЭК на основании оценки работы, защиты, ответов на вопросы (с учётом отзывов руководителя и рецензентов).

**Сведения об авторах (составителях)
ПРОГРАММЫ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ**

Составители:

И.о. зав. кафедрой КЗИ к.т.н.

Д.А. Митюшин

(Должность, уч. степень, уч. звание

подпись

расшифровка подписи)

Лист изменений

В ПРОГРАММЕ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

№ п/п	Дата внесения изменений	Дата и № протокола заседания кафедры	Содержание изменения	Подпись
1.	08.05.2020 г.	Приказ РГГУ от 08.05.2020 № 01-230 осн	<p>Особенности проведения ГИА в 2019/20 учебном году (далее – Особенности) определяют порядок организации и проведения государственной итоговой аттестации аспирантов, завершающих освоение имеющих государственную аккредитацию образовательных программ высшего образования - программ подготовки научно-педагогических кадров в аспирантуре университета (далее – программа аспирантуры), обусловленные мероприятиями, направленными на предотвращение распространения новой коронавирусной инфекции (COVID-19) на территории Российской Федерации.</p> <p>Государственные аттестационные испытания проводятся в следующие сроки: государственный экзамен в период 19 июня по 03 июля 2020 г.; представление научного доклада об основных результатах подготовленной научно-квалификационной работы (диссертации) в период с 01 сентября по 28 сентября 2020 г.</p>	Управление аспирантурой и докторантурой

			<p>Документы, необходимые для представления научного доклада направляются в Управление аспирантурой и докторантурой в электронной форме (документ на бумажном носителе, преобразованный в электронную форму путем сканирования или фотографирования с обеспечением машиночитаемого распознавания его реквизитов) по электронному адресу aspirant_rgggu@rggu.ru</p> <p>Взаимодействие с обучающимися и проведение государственных аттестационных испытаний осуществляется с использованием дистанционных технологий.</p> <p>При проведении государственных аттестационных испытаний обеспечивается идентификация личности обучающегося.</p> <p>Сведения о результатах идентификации обучающегося вносятся в протокол заседания государственной экзаменационной комиссии. В случае невозможности идентификации обучающийся отстраняется от участия в государственном аттестационном испытании. В протокол заседания государственной экзаменационной комиссии вносится запись «неявка по неуважительной причине» в связи с невозможностью идентификации обучающегося.</p>	
--	--	--	--	--

