

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«УФИМСКИЙ ГОСУДАРСТВЕННЫЙ АВИАЦИОННЫЙ ТЕХНИЧЕСКИЙ
УНИВЕРСИТЕТ»

Кафедра вычислительной техники и защиты информации

УТВЕРЖДАЮ
Проректор по учебной работе
Н.Г. Зарипов
«29» 12 2016 г.



ПРОГРАММА государственной итоговой аттестации

выпускников по направлению подготовки

10.03.01 Информационная безопасность

Направленность подготовки (профиль)

Безопасность автоматизированных систем

Уровень подготовки

Высшее образование – бакалавриат

Квалификация

бакалавр

Год начала подготовки – 2015

Уфа 2016

Программа ГИА является приложением к основной профессиональной образовательной программе высшего образования по направлению подготовки 10.03.01 «Информационная безопасность» и профилю «Безопасность автоматизированных систем».

Программа ГИА составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего профессионального образования по направлению подготовки 090900 Информационная безопасность, утвержденного приказом Министерства образования и науки Российской Федерации 28 октября 2009 г. № 496, а также в соответствии с Приказом Министерства образования и науки Российской Федерации от 19 декабря 2013 г. N 1367 г. «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры» и актуализирована в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 Информационная безопасность, утвержденного приказом Министерства образования и науки Российской Федерации 01 декабря 2016 г. № 1515.

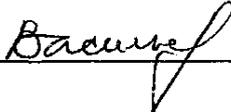
Составитель  В.А. Дуленко

Программа одобрена на заседании кафедры вычислительной техники и защиты информации 26 декабря 2016 г., протокол № 7.

Заведующий кафедрой  В.И. Васильев

Программа ГИА утверждена на заседании НМС по УГСН 10.00.00 Информационная безопасность

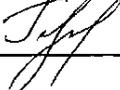
28 декабря 2016 г., протокол № 4.

Председатель НМС  В.И. Васильев

Представители работодателя:

Директор ЗАО «Республиканский центр защиты информации»  С.Н. Зарипов
ФИО, должность, наименование организации



Начальник ООПБС (ООПМА)  Г.Т. Гарипова

1. Общие положения

1. Государственная итоговая аттестация по программе бакалавриата является обязательной для обучающихся, осваивающих программу высшего образования вне зависимости от форм обучения и форм получения образования, и претендующих на получение документа о высшем образовании образца, установленного Министерством образования и науки Российской Федерации.

Целью государственной итоговой аттестации является установление уровня подготовленности обучающегося образовательной организации высшего образования (далее – ООВО), осваивающего образовательную программу бакалавриата (далее – обучающийся), к выполнению профессиональных задач и соответствия его подготовки требованиям федерального государственного образовательного стандарта высшего образования и основной профессиональной образовательной программы высшего образования (далее – ОПОП) по направлению подготовки 10.03.01 «Информационная безопасность», разработанной на основе образовательного стандарта.

Трудоемкость государственной итоговой аттестации в зачетных единицах определяется ОПОП в соответствии с образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 10.03.01 «Информационная безопасность», утвержденный приказом Министерства образования и науки Российской Федерации от 01 декабря 2016 г. № 1515, 9 з.е / 324 часа.

1.1 Государственная итоговая аттестация по направлению подготовки 10.03.01 «Информационная безопасность»

включает:

- а) государственный экзамен;
- б) защиту выпускной квалификационной работы.

2 Требования к выпускнику, проверяемые в ходе государственного экзамена

В рамках проведения государственного экзамена проверяется степень освоения выпускником следующих компетенций:

| Код | Содержание |
|---|--|
| Общепрофессиональные компетенции (ОПК) | |
| ОПК-3 | Способность применять положения электротехники, электроники и схемотехники для решения профессиональных задач |
| ОПК-4 | Способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации |
| ОПК-5 | Способность использовать нормативные правовые акты в профессиональной деятельности |
| ОПК-7 | Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты |
| Профессиональные компетенции (ПК) | |
| ПК-2 | Способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования |
| ПК-8 | Способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов |
| ПК-9 | Способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности |

| | |
|---|--|
| ПК-12 | Способность принимать участие в проведении экспериментальных исследований системы защиты информации |
| ПК-13 | Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации |
| ПК-15 | Способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю |
| Профессионально-специализированные компетенции (ПСК) | |
| ПСК-1 | Способность учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации |
| ПСК-2 | Способность выполнять комплекс задач администрирования подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей |
| ПСК-4 | Способность участвовать в разработке аппаратных и программных средств в составе автоматизированных систем связанных с обеспечением информационной безопасности |

2.1 Перечень основных учебных модулей (дисциплин) образовательной программы или их разделов и вопросов, выносимых для проверки на государственном экзамене

Модуль 1. Организационное и правовое обеспечение информационной безопасности:

1. Функции и основные элементы системы обеспечения информационной безопасности Российской Федерации.
2. Межведомственные и государственные комиссии, создаваемые Президентом Российской Федерации и Правительством Российской Федерации, их основные функции и задачи в обеспечении информационной безопасности России.
3. Правовое регулирование защиты конфиденциальной информации в России.
4. Правовое регулирование защиты персональных данных в России.
5. Организация и правовое обеспечение сертификации и лицензирования в России.
6. Правовое регулирование системы менеджмента информационной безопасности. Основные цели и задачи.
7. Правовое регулирование политики информационной безопасности в организации.
8. Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации.
9. Факторы, влияющие на формирование государственной политики в области обеспечения безопасности автоматизированных систем управления критически важными объектами, и ее основные принципы.
10. Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах.

Модуль 2. Программно-аппаратные средства защиты информации. Защита информационных процессов в компьютерных системах:

1. Семейство Криптон. Основные аппаратные и программные версии. Основные ключевые элементы Криптон. Принципы шифрования. Организация работы в сети.
2. Способы проверки целостности данных. Понятие хэш-функции. Основные стандарты. Хэш-функции с ключом и без ключа. Определение, свойства, примеры. Слабые и сильные хэш-функции
3. Практическая схема шифрования и электронной подписи при использовании асиммет-

ричной криптографии.

4. Структура сертификатов X509. Причины использования. Понятие CRL. Структура взаимодействия и иерархия сертификационных агентств. Аутентификация с помощью сертификатов.

5. Классификация средств вычислительной техники и автоматизированных систем по уровню защищенности от НСД. Показатели защищенности СВТ от НСД. Оценка класса защищенности средств вычислительной техники. Классификация ИСПДн и государственных информационных систем, не обрабатывающих сведения, составляющие государственную тайну.

6. Понятие VPN. Область применения. Основные схемы туннелирования, их особенности. Назначение и использование протоколов семейства IPSEC.

7. Понятие, основные типы межсетевых экранов, их соответствие уровням модели OSI. Принципы работы и особенности. Понятие и виды NAT

8. Файлы и права доступа к ним в Unix. Классификация пользователей по отношению к файлу, ее достоинства и недостатки. Особенности прав доступа файлов и каталогов. Права доступа вновь созданных файлов. Изменение прав доступа при копировании и перемещении.

9. Механизмы и принципы работы файловой системы шифрования (EFS) и подсистемы Bitlocker Windows, особенности реализации в разных версиях Windows.

10. Средства быстрой настройки системы безопасности операционной системы Windows. Понятие групповой политики, порядок наследования и применения групповых политик в Windows Server 2003/2008, связь групп пользователей и групповой политики.

Модуль 3. Техническая защита информации:

1. Принципы и методы технической защиты информации.

2. Основные свойства информации как предмета защиты.

3. Демаскирующие признаки объектов защиты и их классификация.

4. Источники опасных сигналов.

5. Принципы и технология добывания информации. Классификация каналов утечки информации.

6. Акустические каналы утечки информации.

7. Оптические каналы утечки информации.

8. Радиоэлектронные каналы утечки информации.

9. Помехи и их источники.

10. Способы и средства наблюдения.

11. Способы противодействия средствам разведки.

Модуль 4. Сети и системы передачи информации:

1. Как передатчик определяет факт потери положительной квитанции в методе скользящего окна? Сеть с коммутацией пакетов испытывает перегрузку. Для устранения этой ситуации размер окна в протоколах сети нужно увеличить или уменьшить? Как влияет надежность линий связи на выбор размера окна?

2. Опишите функциональное назначение и базовые принципы работы коммуникационного оборудования – повторителей, концентраторов, мостов, коммутаторов, маршрутизаторов.

3. Какая информация хранится в таблицах мостов, коммутаторов и маршрутизаторов? Каким образом информация может попадать в эти таблицы?

4. Что такое домен коллизий в сети Ethernet? Как меняется состав и протяженность домена коллизий при переходе от технологий 10-Base к технологиям 100-Base? За счет каких мер поддерживается достаточно большой размер домена в гигабитном варианте технологии?

5. Каким образом коммутатор Ethernet/Fast Ethernet может управлять потоком кадров, поступающих от сетевых адаптеров рабочих станций сети? Почему необходимость в таком управлении возникает?

6. Каким образом, и с помощью какого оборудования может быть построена крупная ЛВС, состоящая из сегментов, реализованных на основе разных технологий? Как обеспечивается согласованная работа этих разнородных сегментов?

7. Сколько уровней имеет стек протоколов TCP/IP? Каковы их функции? Какие особен-

ности этого стека обуславливают его лидирующее положение в мире сетевых технологий?

8. Какую роль играют протоколы ARP и RARP при реализации стека TCP/IP? В чем заключается типовая последовательность действий по протоколу ARP?

9. В каких случаях, и с каким стеком протоколов используется протокол DHCP? Какова последовательность действий для этого протокола и какую информацию он позволяет получить?

10. В чем заключается различие между видами сервиса, предоставляемыми протоколами UDP и TCP? Как идентифицируются программные объекты в сети на базе стек TCP/IP? Возможно ли обращение к программе, работающей на подключенном к IP-сети компьютере без знания его сетевого адреса?

11. Какие параметры являются основными с точки зрения конфигурирования компьютера с ОС MS Windows для работы в локальной сети? Особое внимание уделите стеку TCP/IP.

12. Приведите примеры протоколов, предназначенных для обеспечения работы маршрутизаторов. Кратко опишите назначение отдельных полей таблицы маршрутизации при использовании в качестве базового протокола IP.

13. Какие подходы наиболее популярны при организации сетевых операционных систем с точки зрения размещения ресурсов, выделяемых в общее пользование? В каких случаях каждый из подходов предпочтителен? Приведите примеры конкретных ОС.

14. Какими факторами определяется в основном пропускная способность информационного канала? Приведите примерную числовую оценку теоретического предела скорости передачи данных в битах в секунду по каналу с шириной полосы в 16 кГц, если амплитуда сигнала передатчика на входе приемника составляет 0,01 мВ, а средняя амплитуда шума в канале 0,0026 мВ? Перечислите и приведите краткую характеристику видов модуляции сигнала при модемной передаче по аналоговым телефонным линиям.

15. Опишите способы реализации дуплексной связи в модемных протоколах. Каким образом в современных модемных протоколах обеспечивается достижение наивысшей скорости обмена по аналоговым телефонным линиям? Какие более современные технологии позволяют существенно повысить скорость передачи по абонентским телефонным линиям и за счет чего?

Модуль 5. Документоведение. Защита и обработка документов ограниченного доступа:

1. Понятие, функции, свойства, признаки документа.

2. Виды документов. Их характеристики.

3. Бланки документов. Виды бланков. Примеры.

4. Формуляр-образец. Основные требования (форматы, поля, координационная сетка, зоны, части, реквизиты).

5. Способы унификации текстов документов. Оформление таблиц, трафаретов, анкет.

6. Система организационно-правовой документации. Назначение, состав, область применения. Цель разработки.

7. Система справочно-информационной документации. Назначение и состав. Область применения. Правила составления и оформления. Пример оформления приказа.

8. Система справочно-аналитической документации. Назначение и состав. Область применения. Правила составления и оформления. Пример оформления докладной записки.

9. Информационные ресурсы государства. Определить понятие «Защищаемая информация». Указать ее виды.

10. Понятие «Конфиденциальный документ». Грифы конфиденциальных документов.

11. Источники конфиденциальной информации и каналы ее разглашения.

12. Понятие «Защищенный документооборот». Требования к нему, принципы организации, структура.

13. Технологические системы обработки и хранения конфиденциальных документов. Требования к ним, виды систем.

14. Перечислить основные требования по организации системы доступа к конфиденциальным документам, сведениям, базам данных.

15. Принципы учета конфиденциальных документов.
16. Технология обработки поступивших конфиденциальных документов.
17. Этапы подготовки конфиденциальных документов.
18. Учет, изготовление и издание конфиденциальных документов.
19. Технология контроля исполнения конфиденциальных документов.
20. Основные требования и порядок проведения проверки наличия конфиденциальных документов, дел и носителей информации.
21. Порядок уничтожения конфиденциальных документов, дел и носителей информации.
22. Формирование и хранение конфиденциальных дел.
23. Основные требования по обращению с конфиденциальными документами при проведении совещаний и переговоров.

2.2 Критерии выставления оценок на государственном экзамене

Результаты государственного экзамена определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» и оформляются протоколами заседаний экзаменационной комиссии.

Ответ по каждому вопросу билета также оценивается на «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Оценки «отлично» заслуживает обучающийся, обнаруживший глубокое и систематическое знание учебно-программного материала по дисциплине, умение выполнить практическое задание в полном объеме, усвоивший взаимосвязь основных понятий дисциплины, проявивший творческие способности в понимании, изложении, использовании учебно-программного материала по данной дисциплине.

Оценки «хорошо» заслуживает обучающийся, обнаруживший хорошее знание учебно-программного материала, умение выполнить практическое задание с не принципиальными ошибками, усвоивший взаимосвязь основных понятий дисциплины, проявивший достаточное понимание при изложении учебно-программного материала по данной дисциплине.

Оценки «удовлетворительно» заслуживает обучающийся, обнаруживший знание учебно-программного материала в неполном объеме, выполнивший практическое задание, но допустивший при этом ряд ошибок; не усвоивший взаимосвязь основных понятий дисциплины, проявивший непонимание в изложении учебно-программного материала по данной дисциплине.

Оценки «неудовлетворительно» заслуживает обучающийся, обнаруживший значительные пробелы в знании учебно-программного материала, не выполнивший практическое задание или допустивший при этом ряд принципиальных ошибок; проявивший непонимание в изложении учебно-программного материала по данной дисциплине.

Окончательная оценка выставляется председателем экзаменационной комиссии на основании среднего арифметического значения оценок, выставленных обучающемуся преподавателями-членами экзаменационной комиссии за ответы на вопросы по отдельным дисциплинам.

В спорных случаях проверяется правильность и аргументация выставленных оценок. По результатам проверки председатель, учитывая мнение членов экзаменационной комиссии, выставляет результирующую оценку.

2.3 Порядок проведения экзамена

К государственному экзамену допускаются лица, завершившие полный курс обучения по образовательной программе и успешно прошедшие все предшествующие аттестационные испытания, предусмотренные учебным планом.

Государственный экзамен проводится по билетам, утвержденным председателем экзаменационной комиссии. Экзамен проводится в письменной форме. Продолжительность экзамена – три астрономических часа.

Каждый экзаменационный билет содержит 5 теоретических вопросов или практических заданий. Вопросы сформулированы с учетом задач, изложенных в рабочих программах дисциплин, выносимых на государственный экзамен, и предусматривают проверку остаточных зна-

ний по разделам и темам, прочитанным в лекционных курсах, рассмотренных на практических и лабораторных занятиях. Фонды экзаменационных вопросов являются неотъемлемой частью настоящей программы и подготовлены выпускающей кафедрой «Вычислительная техника и защита информации».

При ответе на теоретические вопросы обучающийся должен подтвердить соответствие полученных за время обучения знаний знаниям, определяемым ФГОС ВО и учебными программами дисциплин, выносимых на государственный экзамен. При решении задач обучающийся должен показать знание способов и методов их решения.

Результаты экзамена подводятся на заседании экзаменационной комиссии.

В качестве источников информации для подготовки к экзамену используются литература и источники, рекомендованные при изучении соответствующих дисциплин, выносимых на государственный экзамен.

Итоговый государственный экзамен проводится в письменной форме на открытом заседании экзаменационной комиссии по специальности 10.03.01 Информационная безопасность. В состав комиссии входят ведущие преподаватели.

Государственный экзамен проводится в следующем порядке:

- дата и время начала экзамена устанавливаются распоряжением заведующего выпускающей кафедрой, и информация об этом заблаговременно доводится до сведения обучающегося;
- экзамен проводится по билетам, утвержденным председателем комиссии;
- время, отводимое на выполнение экзаменационных заданий, равно 3 астрономическим часам;

- результаты сдачи государственного экзамена объявляются на следующий рабочий день после дня его проведения и оформления в установленном порядке протокола заседания Государственной аттестационной комиссии;

- обучающиеся, не прошедшие государственной итоговой аттестации в связи с неявкой на государственное аттестационное испытание по уважительной причине (временная нетрудоспособность, исполнение общественных или государственных обязанностей, вызов в суд, транспортные проблемы (отмена рейса, отсутствие билетов), погодные условия или в других случаях, перечень которых устанавливается организацией самостоятельно), вправе пройти ее в течение 6 месяцев после завершения государственной итоговой аттестации. Обучающийся должен представить в организацию документ, подтверждающий причину его отсутствия.

3. Требования к выпускной квалификационной работе

По итогам выпускной квалификационной работы проверяется степень освоения выпускником следующих компетенций:

| Код | Содержание |
|---|--|
| Общекультурные компетенции (ОК) | |
| ОК-2 | Способность использовать основы экономических знаний в различных сферах деятельности |
| ОК-5 | Способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики |
| ОК-7 | Способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия |
| ОК-8 | Способность к самоорганизации и самообразованию |
| Общепрофессиональные компетенции (ОПК) | |
| ОПК-1 | Способность анализировать физические явления и процессы для решения профессиональных задач |

| | |
|--|--|
| ОПК-2 | Способность применять соответствующий математический аппарат для решения профессиональных задач |
| ОПК-3 | Способность применять положения электротехники, электроники и схемотехники для решения профессиональных задач |
| ОПК-4 | Способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации |
| ОПК-5 | Способность использовать нормативные правовые акты в профессиональной деятельности |
| ОПК-7 | Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты |
| Профессиональные компетенции (ПК) | |
| ПК-2 | Способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач |
| ПК-4 | Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты |
| ПК-7 | Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений |
| ПК-8 | Способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов |
| ПК-9 | Способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности |
| ПК-10 | Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности |
| ПК-12 | Способность принимать участие в проведении экспериментальных исследований системы защиты информации |
| ПК-13 | Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации |
| ПК-15 | Способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю |
| Профессионально-специализированные компетенции (ПСК) | |
| ПСК-1 | Способность учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации |
| ПСК-2 | Способность выполнять комплекс задач администрирования подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей |
| ПСК-3 | Способность планировать и организовывать комплекс мероприятий по защите информации связанных с обеспечением надежности функционирования и отказоустойчивости аппаратных и программных средств обработки информации |
| ПСК-4 | Способность участвовать в разработке аппаратных и программных средств в составе автоматизированных систем связанных с обеспечением информационной безопасности |

3.1 Вид выпускной квалификационной работы

Выпускная квалификационная работа выполняется в виде бакалаврской выпускной квалификационной работы.

3.2 Структура выпускной квалификационной работ и требования к ее содержанию

Требования к содержанию, объему и структуре выпускной квалификационной работы определяются с учетом требований, изложенных в Порядке проведения государственной итоговой аттестации по программам бакалавриата, программам специалитета и программам магистратуры, утвержденного приказом Министерства образования и науки Российской Федерации от 29 июня 2015 г. № 636.

Выпускная квалификационная работа должна соответствовать видам и задачам профессиональной деятельности выпускника. Она должна быть представлена в форме рукописи с соответствующим иллюстрационным материалом и библиографией.

Документы, входящие в состав ВКР, должны быть оформлены в соответствии с требованиями стандартов на оформление документации и «Инструкции по оформлению выпускных квалификационных работ обучающихся по образовательным программам высшего образования - программам бакалавриата, программам специалитета и программам магистратуры», утвержденной приказом по УГАТУ № 2 272-О от 26.12.2016.

Пояснительная записка к ВКР должна содержать:

1. Титульный лист.
2. Задание по подготовке ВКР.
3. Календарный план работы над ВКР.
4. Аннотация.
5. Содержание.
6. Обозначения и сокращения.
7. Введение.
8. Основная часть.
9. Заключение.
10. Список литературы.
11. Приложения (при необходимости).
12. Отзыв руководителя.
13. Акты внедрения (при наличии).
14. Справка о результатах проверки ВКР на плагиат.
15. Рецензия на ВКР (вкладывается во вшитый файл).
16. Печатный вариант презентационного материала (вкладывается во вшитый файл).

Титульный лист ВКР, задание на ВКР, календарный план и другие составные части пояснительной записки оформляются в соответствии с действующими нормативными актами.¹

Аннотация – краткая характеристика документа с точки зрения его назначения, содержания, вида, формы и других особенностей. Аннотация используется в качестве элемента библиографической записи и элемента выходных сведений.

Аннотация оформляется на отдельной странице без правил оформления, предусмотренных ГОСТ 2.104-2006. Рекомендуемый средний объем аннотации 500 печатных знаков. Объем аннотации не должен превышать одной печатной страницы.

Аннотация должна содержать:

- сведения об объеме ВКР, количестве иллюстраций, таблиц, приложений, количестве частей ВКР, количестве использованных источников;
- перечень ключевых слов;
- текст аннотации.

Аннотации на разных языках оформляются каждая на отдельной странице.

¹ «Инструкции по оформлению выпускных квалификационных работ обучающихся по образовательным программам высшего образования - программам бакалавриата, программам специалитета и программам магистратуры», утвержденной приказом по УГАТУ № 2 272-О от 26.12.2016.

Перечень ключевых слов должен включать от 5 до 15 слов или словосочетаний из текста ВКР, которые в наибольшей мере характеризуют его содержание и обеспечивают возможность информационного поиска. Ключевые слова приводятся в именительном падеже и печатаются строчными буквами в строку через запятые.

Содержание представляет собой перечень номеров и наименований всех основных элементов текста ВКР с указанием номеров страниц, с которых начинаются эти элементы. Первый лист содержания размещается на листе со штампом по форме 2 согласно ГОСТ 2.104-2006, т.к. является заглавным листом пояснительной записки. Наименования, включенные в содержание, записывают строчными буквами, начиная с прописной. Выравнивание текста содержания осуществляется по левому краю без абзацного отступа. Наименования заголовков и подзаголовков отделяются от номера соответствующей страницы отточиями.

Структурный элемент «*Обозначения и сокращения*» представляет собой перечень условных сокращений, использованных в тексте ВКР. Данный раздел приводится в случае использования в тексте ВКР более пяти сокращений. Сокращения русских слов выполняются в соответствии с ГОСТ Р 7.0.12-2011, сокращения иностранных слов – в соответствии с ГОСТ 7.11-2004. Перечень сокращений формируется в алфавитном порядке. При наличии англоязычных сокращений после их раскрытия в скобках дается русскоязычная трактовка.

Введение представляет собой подраздел пояснительной записки ВКР, в котором, как правило, указываются следующие элементы:

- актуальность тематики;
- цель и задачи работы;
- объект и предмет исследования;
- теоретические основы, метод или методология проведения работы (исследования) и необходимые технические средства;
- теоретическая и/или практическая значимость работы;
- научная новизна и апробация работы;
- характеристика структуры работы.

Основная часть пояснительной записки ВКР должна содержать разделы, подразделы, пункты, отражающие содержание и результаты выполненной работы. Она включает в себя следующие составляющие:

Основная часть ВКР должна содержать реферативную часть, отражающую общую профессиональную эрудицию автора, а также самостоятельную исследовательскую часть, выполненную индивидуально или в составе творческого коллектива по материалам, собранным или полученным самостоятельно студентом в период прохождения производственной практики и научно-исследовательской работы.

Самостоятельная часть ВКР должна быть законченным исследованием, свидетельствующим об уровне профессиональных компетенций автора. Требования к содержанию, объему и структуре ВКР определяются вузом на основании действующего Положения об итоговой государственной аттестации выпускников вузов и методических рекомендаций УМО по направлению подготовки «Информационная безопасность».

Заключение (выводы), входящие в состав пояснительной записки ВКР должно содержать анализ результатов теоретических, расчетных работ, экспериментальных исследований (при наличии), опытно-конструкторских работ (при наличии), проведенных обучающимся при выполнении ВКР, и рекомендации по их практическому применению. При этом должны быть обозначены результаты, полученные обучающимися самостоятельно.

Список литературы должен содержать библиографическое описание всех литературных источников, использованных в процессе подготовки ВКР. Список необходимо оформлять в соответствии с требованиями ГОСТ 7.1-2003 и ГОСТ 7.82-2001. На все источники, указанные в списке литературы, должны быть ссылки в тексте ВКР.

В *приложении* к ВКР могут быть помещены следующие элементы:

- чертежи;

- листинги и скриншоты компьютерных программ; таблицы, рисунки и схемы большого формата;
- описания применяемого в работе нестандартного оборудования;
- протоколы испытаний;
- дополнительные расчеты;
- промежуточные математические доказательства, формулы и расчеты;
- описание аппаратуры и приборов, применяемых при проведении экспериментов, измерений и испытаний;
- любой другой материал, дополняющий ВКР.

Все приложения должны быть перечислены в Содержании ВКР с указанием их буквенных обозначений, заголовков и номеров страниц, с которых они начинаются.

Отзыв руководителя ВКР подшивается вместе с пояснительной запиской.

Справка о результатах проверки ВКР на плагиат составляется в соответствии с Порядком проверки выпускных квалификационных работ на объем заимствования, выявления неправомерных заимствований и размещения в электронно-библиотечной системе Университета.

Внешнее рецензирование ВКР проводится ведущими специалистами по тематике ВКР, не являющимися работниками Университета.

3.3 Примерная тематика и порядок утверждения тем выпускных квалификационных работ

Тематика и содержание ВКР должны соответствовать уровню компетенций, полученных выпускником в объеме дисциплин ОПОП.

Темы ВКР могут быть предложены кафедрами или самими обучающимися. В их основе могут быть материалы научно-исследовательских или научно-производственных работ кафедры, факультета, научных или производственных организаций.

Обучающийся по согласованию с руководителем определяет тему ВКР, которая рассматривается на заседании кафедры и утверждается на заседании Ученого совета факультета.

Примерная тематика выпускных квалификационных работ:

1. Система обнаружения возможных каналов утечки сведений, относящихся к конфиденциальной информации.
2. Оценка параметров полей объектов с целью выявления угроз информационной безопасности.
3. Оценка состояния акустической защищенности помещений на предмет их звукоизоляции, инфразвук, ультразвук.
4. Организация защиты информации на предприятии на основе снижения демаскирующих признаков объектов защиты.
5. Оценка надежности системы ограничения доступа в АСУ.
6. Защита информационных ресурсов предприятия (организации) при проведении электронных торгов.
7. Модель комплексной системы защиты информации на предприятии (в организации).
8. Система контроля функционирования комплексной системы защиты информации.
9. Управление комплексной системой защиты информации предприятия в условиях чрезвычайных ситуаций.
10. Защита информации в системе поддержки принятия решения по отбору персонала.
11. Системный анализ информационной инфраструктуры предприятия (на конкретном примере).
12. Система защиты информации учреждения здравоохранения на основе типовых решений.
13. Организация системы защиты электронного документооборота хозяйствующего субъекта (на конкретном примере) на основе применения электронной цифровой подписи.
14. Методика разработки комплексной модели нарушителя режима информационной безопасности для предприятия.

15. Комплексный анализ угроз и уязвимостей информационной системы хозяйствующего субъекта (на конкретном примере) на основе метода многофакторного анализа.
16. Концепция (политика) информационной безопасности хозяйствующего субъекта.
17. Организация комплекса мероприятий по лицензированию объекта информационной системы хозяйствующего субъекта (на конкретном примере) в области защиты информации.
18. Организация комплекса мероприятий по сертификации объекта информационной системы хозяйствующего субъекта (на конкретном примере) в области защиты информации.
19. Организация подбора и подготовки персонала для службы информационной безопасности хозяйствующего субъекта (на конкретном примере).
20. Оценка защищенности технических средств и систем хозяйствующего субъекта (на конкретном примере), предназначенных для обработки конфиденциальной информации от утечки по линиям связи.
21. Оценка защищенности конфиденциальной информации хозяйствующего субъекта (на конкретном примере) от утечки за счет наводок на технические средства, системы и их коммуникации линиям связи.
22. Комплексная оценка защищенности помещения хозяйствующего субъекта (на конкретном примере) от утечки конфиденциальной информации по техническим каналам.
23. Организация комплекса мероприятий по обнаружению и поиску временно отключенных устройств несанкционированного съема информации в защищаемом помещении хозяйствующего субъекта (на конкретном примере).
24. Программная защита информационной системы хозяйствующего субъекта (на конкретном примере) на основе встроенных возможностей современных операционных систем (на конкретном примере).
25. Программная защита информации хозяйствующего субъекта (на конкретном примере) на основе возможностей современных пользовательских приложений (на конкретном примере).
26. Защита информации в локальной (корпоративной) вычислительной сети хозяйствующего субъекта (на конкретном примере) на основе использования возможностей провайдеров.
27. Система антивирусной защиты информационной инфраструктуры хозяйствующего субъекта (на конкретном примере) на основе оценки отечественного и зарубежного рынка.
28. Методика проведения комплексного аудита информационной системы хозяйствующего субъекта (на конкретном примере) с позиций безопасности на основе использования специального программного обеспечения.
29. Организация и применение технологии активного аудита при проведении комплексного аудита информационной системы хозяйствующего субъекта (на конкретном примере) с позиций безопасности.
30. Методика использования тестирующего программного обеспечения (на конкретном примере) при проведении аудита информационной системы хозяйствующего субъекта с позиций безопасности.
31. Разработка аппаратной и программной части криптоплаты.
32. Разработка системы прозрачного шифрования файлов.
33. Разработка корпоративной системы программного шифрования файлов.
34. Разработка системы обеспечения целостности информации с использованием криптографии с открытыми ключами.
35. Оптимизация реализации алгоритмов эллиптической криптографии.
36. Использование гиперэллиптических кривых в системах криптографической защиты.
37. Реализация корпоративной системы открытых ключей.
38. Практическая реализация протокола IPSec.
39. Разработка стеганографической программы с повышенной степенью сокрытия информации.
40. Разработка системы защиты авторских прав с использованием водяных цифровых знаков.

41. Разработка системы разграничения доступа с использованием электронных таблеток iButton.
42. Разработка системы биометрической аутентификации по голосу (клавиатурному почерку, рукописному почерку).
43. Реализация защиты программного обеспечения на электронных ключах с использованием функций API из Developer Kit.
44. Защита DVD электронных учебников от несанкционированного копирования.
45. Защита компьютерных данных от несанкционированного копирования с помощью технологий RMS и IRM.
46. Разработка методики исследования программ с помощью отладчика.
47. Разработка программной системы защиты от кражи ПК.
48. Администрирование Active Directory.
49. Средства управления ролями фирмы Quest Software.
50. Управление групповой политикой корпоративной сети.
51. Реализация защищенного доступа к СУБД на примере SQL Server 2008 (MySQL, PostgreSQL; Oracle).
52. Организация защиты информации в сетях Macintosh.
53. Анализ средств реализации защищенных распределенных систем на базе платформы Linux|Unix.
54. Защита корпоративных сетей на платформе Linux со стороны атак инсайдеров.
55. Реализация защищенных сетей с доменом Active Directory и рабочими станциями Linux.
56. Реализация корпоративной инфраструктуры открытых ключей системы сертификационных агентств на базе Linux/Unix.
57. Управление и настройка аутентификации на основе протокола Kerberos в сетях Linux, Windows и гетерогенных сетях.
58. Защищенные системы комплексного управления и администрирования корпоративных сетей на базе Microsoft Security Center.
59. Разработка защищенного портала предприятия на базе Microsoft SharePoint Server.
60. Проектирование защищенной распределенной корпоративной сети на базе линейки ViPNet фирмы «Инфотекс» (комплекса «Континент» фирмы «Информзащита», продуктов фирмы Cisco, продуктов «Застава» фирмы «Элвис-плюс»).
61. Атаки и защита DNS-серверов.
62. Построение защищенных Web-приложений на основе IIS 6.0 и MS SQL Server.
63. Организация защищенной почтовой системы.
64. Организация защищенных систем электронной торговли.
65. Обеспечение безопасности IP телефонии.
66. Реализация обманных систем и систем-ловушек на базе виртуальных машин.

3.4 Порядок выполнения и представления в государственную экзаменационную комиссию выпускной квалификационной работы

ВКР выполняется под руководством опытного специалиста. Руководители ВКР назначаются из числа профессоров, доцентов, преподавателей, научных сотрудников и высококвалифицированных специалистов университета, других учебных заведений, учреждений и предприятий.

Руководитель ВКР:

- выдает задание на выпускную работу, по установленной форме, с указанием сроков промежуточного контроля и даты представления на кафедру завершенной выпускной работы;
- оказывает студенту помощь в разработке календарного графика работы на весь период написания выпускной работы;
- рекомендует студенту необходимую литературу, справочные и архивные материалы и другие источники по теме;

- проводит систематические, предусмотренные расписанием, консультации;
- проверяет выполнение работы по частям и в целом.

На первом этапе подготовки ВКР руководитель рассматривает и корректирует план работы и дает рекомендации по списку литературы.

В ходе выполнения работы руководитель ВКР является консультантом, указывая выпускнику на недостатки аргументации, композиции, стиля и т.д., а также рекомендует, как их лучше устранить.

Законченная бакалаврская работа, подписанная студентом, предоставляется научному руководителю. После просмотра и одобрения работы руководитель подписывает ее и вместе со своим письменным отзывом представляет заведующему кафедрой. В отзыве должна быть характеристика проделанной студентом работы по всем разделам.

Выпускная работа направляется на рецензию. Состав рецензентов выбирается из числа специалистов учреждений, производства, других высших учебных заведений, а также из числа преподавателей университета, если они не работают на данной выпускающей кафедре. Состав рецензентов утверждается распоряжением ректора УГАТУ.

В случае, если заведующий кафедрой, исходя из содержания отзывов руководителя и рецензента, не считает возможным допустить студента к защите ВКР в ГАК, этот вопрос рассматривается с участием руководителя и автора ВКР.

В случае, если по уважительным причинам (с представлением соответствующих документов) ВКР не готова к защите, по решению заведующего кафедрой ВТиЗИ защита может быть перенесена на более поздний срок.

Если работа готова к защите, заведующий кафедрой на основании письменных отзывов руководителя выпускной работы и рецензента утверждает работу, делая об этом соответствующую запись на титульном листе выпускной работы.

В государственную аттестационную комиссию (ГАК) представляется пояснительная записка, к которой прилагаются:

- выписка из решения выпускающей кафедры о допуске к защите с указанием даты;
- отзыв научного руководителя;
- рецензия с подписью рецензента;
- электронные копии всех документов представляемых на защиту.

В ГАК могут быть представлены также другие материалы, характеризующие научную и практическую ценность выполненной работы: печатные статьи и авторские свидетельства по теме проекта, документы, указывающие на практическое применение результатов работы, демонстрационные ролики.

Обучающийся может (по его желанию и при рекомендации кафедры) представить дополнительное краткое содержание выпускной работы на одном из иностранных языков, которое оглашается на защите и может сопровождаться вопросами к студенту на том же языке.

3.5 Порядок защиты выпускной квалификационной работы

Сроки проведения ГИА в соответствии с утвержденным графиком учебного процесса: 43-44 неделя.

Защита выпускной работы бакалавра осуществляется на заседании Государственной аттестационной комиссии в форме авторского доклада, на который отводится не более 5-7 минут.

Доклад сопровождается презентацией основных положений работы с помощью современных мультимедийных средств отображения информации.

В своем выступлении на заседании ГАК выпускник должен отразить:

- актуальность темы;
- цель и задачи исследования;
- основные положения, на которых базируется ВКР;
- результаты проведенного анализа изучаемого явления;
- конкретные предложения по решению проблемы или совершенствованию соответствующих моделей, процессов и т.п.

В процессе защиты обучающийся должен ответить на заданные вопросы, а также замечания, отмеченные в отзыве руководителя и рецензии.

При оценке ВКР учитывается ее содержание, отзыв руководителя, отзыв и оценка рецензента и результаты защиты.

При положительной оценке ВКР комиссией выставляется оценка «удовлетворительно», «хорошо» или «отлично». Оценка регистрируется в протоколе заседания ГАК.

При неудовлетворительной оценке ВКР, а также при неявке автора на защиту по уважительной (подтвержденной документально) причине, возможно назначение дополнительного срока защиты.

Выпускные работы, прошедшие защиту, хранятся в архиве университета в течение установленного срока.

В тех случаях, когда защита ВКР признается неудовлетворительной, ГАК устанавливает, может ли обучающийся представить к повторной защите тот же проект с доработкой, определяемой комиссией, или же обязан разработать новую тему, которая устанавливается выпускающей кафедрой. Обучающийся, не защитивший ВКР, допускается к повторной защите в течение трех лет после окончания вуза.

После окончания закрытого совещания председатель ГАК зачитывает распоряжение о результатах защиты ВКР.

Выпускные работы, прошедшие защиту, хранятся в архиве университета в течение установленного срока.

Лицо, не прошедшее государственную итоговую аттестацию, может повторно пройти государственную итоговую аттестацию не ранее чем через год и не позднее чем через пять лет после срока проведения государственной итоговой аттестации, которая не пройдена обучающимся.

Для повторного прохождения государственной итоговой аттестации указанное лицо по его заявлению восстанавливается в организации на период времени, установленный организацией, но не менее периода времени, предусмотренного календарным учебным графиком для государственной итоговой аттестации по соответствующей образовательной программе.

При повторном прохождении государственной итоговой аттестации по желанию обучающегося решением организации ему может быть установлена иная тема выпускной квалификационной работы.

По результатам государственных аттестационных испытаний обучающийся имеет право подать в апелляционную комиссию письменную апелляцию о нарушении, по его мнению, установленной процедуры проведения государственного аттестационного испытания и (или) несогласии с результатами государственного экзамена.

Апелляция подается лично обучающимся в апелляционную комиссию не позднее следующего рабочего дня после объявления результатов государственного аттестационного испытания.

3.6 Критерии выставления оценок (соответствия уровня подготовки выпускника требованиям ФГОС ВО)

| № п.п. | Разделы (части) работы | Критерии оценки | | | |
|--------|---|---|--|---|--|
| | | <i>отлично</i> | <i>хорошо</i> | <i>удовлетворительно</i> | <i>неудовлетворительно</i> |
| 1 | Качество квалификационной работы оценивается членами ГАК по составляющим:* | | | | |
| 1 | <i>обоснованность актуальности проблемы</i> исследования и темы работы – предполагает оценку степени убедительности оснований, побудивших обучающегося выбрать данную проблему для изучения на определенном объекте исследования | <i>обоснованность актуальности проблемы</i> исследования и темы работы <i>полностью соответствует</i> предъявляемым требованиям | <i>обоснованность актуальности проблемы</i> исследования и темы работы <i>в основном соответствует</i> предъявляемым требованиям | <i>обоснованность актуальности проблемы</i> исследования и темы работы <i>частично соответствует</i> состоянию по конкретному параметру | <i>обоснованность актуальности проблемы</i> исследования и темы работы <i>не соответствует</i> предъявляемым требованиям |
| 2 | <i>уровень теоретической проработки</i> проблемы предполагает оценку широты и качества изученных литературных источников, логики изложения материала, глубины обобщений и выводов в первой главе, а также теоретического обоснования возможных решений проблемы | <i>уровень теоретической проработки полностью соответствует</i> предъявляемым требованиям | <i>уровень теоретической проработки работы в основном соответствует</i> предъявляемым требованиям | <i>уровень теоретической проработки частично соответствует</i> состоянию по конкретному параметру | <i>уровень теоретической проработки не соответствует</i> предъявляемым требованиям |
| 3 | <i>методическая грамотность проведенных исследований</i> предполагает оценку обоснованности применения методик исследования, информационной адекватности и правильности использования конкретных методов и методик анализа | <i>методическая грамотность проведенных исследований полностью соответствует</i> предъявляемым требованиям | <i>методическая грамотность проведенных исследований в основном соответствует</i> предъявляемым требованиям | <i>методическая грамотность проведенных исследований частично соответствует</i> состоянию по конкретному параметру | <i>методическая грамотность проведенных исследований не соответствует</i> предъявляемым требованиям |

| | | | | | |
|---|---|--|---|--|---|
| 4 | <i>достаточность и качество обоснования</i> предлагаемых управленческих (технических) решений предполагает оценку адекватности выбранных методов обоснования решений, правильность их применения | <i>достаточность и качество обоснования</i> предлагаемых управленческих (технических) решений <i>полностью соответствует</i> предъявляемым требованиям | <i>достаточность и качество обоснования</i> предлагаемых управленческих (технических) решений <i>в основном соответствует</i> предъявляемым требованиям | <i>достаточность и качество обоснования</i> предлагаемых управленческих (технических) решений <i>частично соответствует</i> состоянию по конкретному параметру | <i>достаточность и качество обоснования</i> предлагаемых управленческих (технических) решений <i>не соответствует</i> предъявляемым требованиям |
| 5 | <i>полнота раскрытия темы ВКР</i> , соответствие темы ВКР ее содержанию, наличие публикаций по теме исследования, апробация результатов исследования (наличие актов, справок о внедрении) | <i>полнота раскрытия темы ВКР полностью соответствует</i> предъявляемым требованиям | <i>полнота раскрытия темы ВКР в основном соответствует</i> предъявляемым требованиям | <i>полнота раскрытия темы ВКР частично соответствует</i> состоянию по конкретному параметру | <i>полнота раскрытия темы ВКР не соответствует</i> предъявляемым требованиям |
| 6 | <i>практическая значимость выполненной работы</i> предполагает оценку возможности практического применения результатов исследования в деятельности конкретной организации или в сфере возможной профессиональной занятости выпускников в соответствии с требованиями ФГОС ВО | <i>практическая значимость выполненной работы полностью соответствует</i> предъявляемым требованиям | <i>практическая значимость выполненной работы в основном соответствует</i> предъявляемым требованиям | <i>практическая значимость выполненной работы частично соответствует</i> состоянию по конкретному параметру | <i>практическая значимость выполненной работы не соответствует</i> предъявляемым требованиям |
| 7 | <i>качество оформления квалификационной работы</i> предполагает оценку на соответствие стандартам, а также аккуратность и выразительность оформления материала, грамотность и правильность подготовки сопроводительных документов, наличие и качество подготовки раздаточного материала | <i>качество оформления квалификационной работы полностью соответствует</i> предъявляемым требованиям | <i>качество оформления квалификационной работы в основном соответствует</i> предъявляемым требованиям | <i>качество оформления квалификационной работы частично соответствует</i> состоянию по конкретному параметру | <i>качество оформления квалификационной работы не соответствует</i> предъявляемым требованиям |

| | | | | | | |
|---|---|--|--|---|--|---|
| 2 | Качество выступления на защите квалификационной работы оценивается членами ГАК по следующим составляющим | | | | | |
| 3 | 1 | <i>качество доклада</i> предполагает оценку соответствия доклада содержанию работы, способности выпускника выделить научную и практическую ценность выполненных исследований, умения пользоваться иллюстративным материалом, средствами мультимедийной презентации | <i>качество оформления квалификационной работы полностью соответствует</i> предъявляемым требованиям | <i>качество оформления квалификационной работы в основном соответствует</i> предъявляемым требованиям | <i>качество оформления квалификационной работы частично соответствует</i> состоянию по конкретному параметру | <i>качество оформления квалификационной работы не соответствует</i> предъявляемым требованиям |
| | 2 | <i>качество ответов на вопросы</i> предполагает оценку правильности, четкости, полноты и обоснованности ответов выпускника, умения лаконично и точно сформулировать свои мысли, используя при этом необходимую научную терминологию | <i>качество ответов на вопросы соответствует</i> предъявляемым требованиям | <i>качество ответов на вопросы в основном соответствует</i> предъявляемым требованиям | <i>качество ответов на вопросы частично соответствует</i> состоянию по конкретному параметру | <i>качество ответов на вопросы не соответствует</i> предъявляемым требованиям |
| | 3 | <i>качество иллюстраций</i> к докладу предполагает оценку соответствию подбору иллюстративных материалов содержанию доклада, грамотность их оформления и упоминания в докладе, выразительность использованных средств графического и художественного воплощения | <i>качество иллюстраций к докладу соответствует</i> предъявляемым требованиям | <i>качество иллюстраций к докладу в основном соответствует</i> предъявляемым требованиям | <i>качество иллюстраций к докладу частично соответствует</i> состоянию по конкретному параметру | <i>качество иллюстраций к докладу не соответствует</i> предъявляемым требованиям |

| | | | | | | |
|--|---|--|---|--|---|--|
| | 4 | <i>поведение при защите квалификационной работы</i> предполагает оценку коммуникационных характеристик докладчика (манера говорить, отстаивать свою точку зрения, привлекать внимание к важным моментам в докладе или ответах на вопросы и т.д.) | <i>поведение при защите квалификационной работы соответствует</i> предъявляемым требованиям | <i>поведение при защите квалификационной работы в основном соответствует</i> предъявляемым требованиям | <i>поведение при защите квалификационной работы частично соответствует</i> состоянию по конкретному параметру | <i>поведение при защите квалификационной работы не соответствует</i> предъявляемым требованиям |
| | 4 | Оценка выпускной квалификационной работы рецензентом и его рекомендации по присвоению выпускнику квалификации «специалист» переносятся из рецензии, подписанной рецензентом | <i>ВКР соответствует</i> предъявляемым требованиям | <i>ВКР в основном соответствует</i> предъявляемым требованиям | <i>ВКР частично соответствует</i> состоянию по конкретному параметру | <i>ВКР не соответствует</i> предъявляемым требованиям |
| | 5 | Оценка научным руководителем выпускной квалификационной работы и его рекомендации по присвоению выпускнику квалификации «специалист» переносятся из отзыва руководителя | <i>ВКР соответствует</i> предъявляемым требованиям | <i>ВКР в основном соответствует</i> предъявляемым требованиям | <i>ВКР частично соответствует</i> состоянию по конкретному параметру | <i>ВКР не соответствует</i> предъявляемым требованиям |

Снятие ВКР с защиты возможно в случае несоответствия темы представленной на защиту работы утвержденному списку тем, в случае выявления плагиата или несоответствие содержания ВКР направлению подготовки.

Итоговая оценка выпускной квалификационной работы определяется усреднением оценок членов ГАК.

Наряду с определением итоговой оценки, ГАК может вынести:

- рекомендации ВКР к опубликованию и участию в конкурсах студенческих работ;
- рекомендации ВКР к расширенному использованию (практическое использование, внедрение результатов в образовательный процесс).

4 Проведение ГИА для лиц с ОВЗ

Проведение ГИА для обучающихся инвалидов и лиц с ОВЗ осуществляется с учетом рекомендованных условий обучения для инвалидов и лиц с ОВЗ. В таком случае требования к процедуре проведения и подготовке итоговых испытаний должны быть адаптированы под конкретные ограничения возможностей здоровья обучающегося, для чего должны быть предусмотрены специальные технические условия.

