

МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

декан факультета прикладной
математики, информатики
и механики

А.И. Шашкин

26.05.2020



**ПРОГРАММА
ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ**

1. Код и наименование направления подготовки/специальности:

10.05.01 Компьютерная безопасность

2. Профиль подготовки/специализация:

математические методы защиты информации

3. Квалификация выпускника: Специалист по защите информации

4. Форма(ы) обучения: очная

5. Утверждена Учёным советом факультета прикладной математики, информатики и механики (протокол № 6 от 26.05.2020).

6. Учебный год: 2025/2026

7. Цель государственной итоговой аттестации: определение соответствия результатов освоения обучающимися основной образовательной программы «Математические методы защиты информации» соответствующим требованиям ФГОС по направлению подготовки/специальности 10.05.01 Компьютерная безопасность, утвержденный приказом Минобрнауки от 01.12.2016 № 1512.

8. Место государственной итоговой аттестации в структуре ООП: Блок БЗ, базовая часть

9. Форма(ы) государственной итоговой аттестации:

- Подготовка к защите и защита выпускной квалификационной работы.

10. Планируемые результаты освоения образовательной программы (компетенции выпускников):

Код	Название
Общекультурные компетенции	
ОК-1	способностью использовать основы философских знаний для формирования мировоззренческих позиций
ОК-2	способностью использовать основы экономических знаний в различных сферах деятельности
ОК-3	способностью анализировать основные этапы и закономерности исторического развития России, ее место и роль в современном мире для формирования гражданской позиции и развития патриотизма
ОК-4	способностью использовать основы правовых знаний в различных сферах деятельности
ОК-5	способностью понимать социальную значимость своей 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-6	способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия
ОК-7	способностью к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности
ОК-8	способностью к самоорганизации и самообразованию
ОК-9	способностью использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности
Общепрофессиональные компетенции	
ОПК-1	способностью анализировать физические явления и процессы при решении профессиональных задач
ОПК-2	способностью корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов
ОПК-3	способностью понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и иных источниках информации
ОПК-4	способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами

ОПК-5	способностью использовать нормативные правовые акты в своей профессиональной деятельности
ОПК-6	способностью применять приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций
ОПК-7	способностью учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения
ОПК-8	способностью использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач
ОПК-9	способностью разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации
ОПК-10	способностью к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах
Профессиональные компетенции	
ПК-1	способностью осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности
ПК-2	способностью участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах, составлять научные отчеты, обзоры по результатам выполнения исследований
ПК-3	способностью проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности
ПК-4	способностью проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем
ПК-5	способностью участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации
ПК-6	способностью участвовать в разработке проектной и технической документации
ПК-7	способностью проводить анализ проектных решений по обеспечению защищенности компьютерных систем
ПК-8	способностью участвовать в разработке подсистемы информационной безопасности компьютерной системы
ПК-9	способностью участвовать в проведении экспериментально-исследовательских работ при аттестации объектов с учетом требований к уровню защищенности компьютерной системы
ПК-10	способностью оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации
ПК-11	способностью участвовать в проведении экспериментально-исследовательских работ при проведении сертификации средств защиты информации в компьютерных системах по требованиям безопасности информации
ПК-12	способностью проводить инструментальный мониторинг защищенности компьютерных систем

ПК-13	способностью организовывать работу малых коллективов исполнителей, находить и принимать управленческие решения в сфере профессиональной деятельности
ПК-14	способностью организовывать работы по выполнению режима защиты информации, в том числе ограниченного доступа
ПК-15	способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы
ПК-16	способностью разрабатывать проекты нормативных правовых актов и методические материалы, регламентирующие работу по обеспечению информационной безопасности компьютерных систем
ПК-17	способностью производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение
ПК-18	способностью производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации
ПК-19	способностью производить проверки технического состояния и профилактические осмотры технических средств защиты информации
ПК-20	способностью выполнять работы по восстановлению работоспособности средств защиты информации при возникновении нештатных ситуаций
Профессионально-специализированные компетенции	
ПСК-2.1	способностью разрабатывать вычислительные алгоритмы, реализующие современные математические методы защиты информации
ПСК-2.2	способностью на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах
ПСК-2.3	способностью строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов
ПСК-2.4	способностью разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации
ПСК-2.5	способностью проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных средств защиты информации с учетом современных и перспективных математических методов защиты информации

11. Объем государственной итоговой аттестации в зачетных единицах / ак. час. – 4/216:

– Подготовка к защите и защита выпускной квалификационной работы – _4/216.

12. Государственный экзамен

Не предусмотрен.

13 Требования к ВКР

13.1. Порядок выполнения ВКР

Выпускная квалификационная работа – вид итогового аттестационного испытания выпускников ВГУ по направлению подготовки 10.05.01 Компьютерная безопасность (специалист), предусмотренная федеральным государственным образовательным стандартом высшего профессионального образования, выполняется в форме выпускной квалификационной работы.

Подготовка ВКР выполняется обучающимся на протяжении заключительного года обучения, является проверкой качества полученных теоретических знаний, практических умений и навыков, сформированных общекультурных и профессиональных компетенций, позволяющих решать профессиональные задачи.

Утверждение тем ВКР, назначение руководителей, организация выполнения ВКР определяется требованиями, изложенными в Положении о порядке проведения государственной итоговой аттестации по образовательным программам высшего образования – программам бакалавриата, программам специалитета и программам магистратуры воронежского государственного университета П ВГУ 2.1.28 – 2018.

К защите ВКР допускается обучающийся, успешно завершивший в полном объеме освоение ООП в соответствии с учебным планом, полностью выполнивший задание кафедры на выполнение ВКР.

Темы работ утверждаются Ученым советом факультета прикладной математики, информатики и механики по представлению заведующих кафедрами. Перечень тем ВКР доводится до сведения обучающихся не позднее, чем за 6 месяцев до ГИА.

Перечень примерных тем бакалаврских работ разрабатывается преподавателями выпускающей кафедры. Примерная тематика бакалаврских работ обсуждается на заседании выпускающей кафедры и утверждается заведующим кафедрой.

Задание на выполнение ВКР выдается студенту после утверждения темы Ученым советом факультета прикладной математики, информатики и механики.

Если тематика выпускной квалификационной работы предполагает использование материалов и методов исследования из других областей знания, то по решению Ученого совета обучающемуся может быть назначен консультант.

К защите ВКР допускается обучающийся, успешно завершивший в полном объеме освоение ООП в соответствии с учебным планом и полностью выполнивший задание на выполнение ВКР.

13.2. Примерный перечень тем ВКР

1. Разработка отказоустойчивой модели корпоративной информационной платформы мобильного оператора;
2. Разработка отказоустойчивой, защищённой модели корпоративного центра обработки данных;
3. Разработка клиент-серверного решения аудита распределённой вычислительной сети;
4. Виртуальная реальность;
5. Медицинские информационные системы;
6. Оперативная аналитическая обработка информации;
7. Разработка обучающей компьютерной программы «Криптосистема Эль Гамала»;
8. Алгоритмы ЗИ в распределённых управляющих системах;
9. Криптоанализ системы шифрования RSA;
10. Информационная безопасность ERP-систем;
11. Разработка защищённой модели корпоративного портала оператора связи;
12. Построение защищённой модели вычислительного кластера в облаке;

13. Моделирование отказоустойчивости и переполнения сетевого стека сервера базы данных;
14. Современные методы моделирования пропускной способности распределённой вычислительной сети;
15. Разработка алгоритма и программы постквантовой криптографии;
16. Алгоритмы ЗИ в ERP-системах;
17. Математические методы криптографии;
18. Разработка программного обеспечения и способов администрирования информационных систем и сетей.
19. Разработка программного обеспечения средств вычислительной техники и автоматизированных систем.
20. Создание и применение средств математического обеспечения информационных систем.
21. Проектирование и разработка информационных систем с применением современных СУБД.
22. Проектирование и разработка веб-приложений для различных сфер профессиональной деятельности.
23. Проектирование и разработка статических и динамических сайтов.

13.3. Структура ВКР

ВКР содержит совокупность результатов и научных положений, выдвигаемых автором для публичной защиты, и свидетельствует о способностях автора проводить самостоятельные научные исследования, опираясь на теоретические знания и практические навыки.

Структура ВКР в форме выпускной квалификационной работы должна включать следующие разделы:

- титульный лист;
- содержание;
- введение;
- основная часть (постановка задачи и разделы основной части);
- заключение;
- список использованных источников (литературы);
- приложения.

Титульный лист должен быть оформлен в соответствии с СТП ВГУ.

Во введении обосновывается актуальность выбранной темы, формулируется цель исследования и задачи, которые необходимо решить для ее достижения; определяются объект и предмет исследования, кратко описывается структура работы.

Основная часть ВКР включает главы, раскрывающие содержание работы и включающее описание научных результатов, полученных в процессе исследования.

В заключении дается анализ полученных результатов, формулируются выводы и рекомендации.

Список использованных источников (не менее 10) должен содержать сведения о публикациях, которые использовались при написании ВКР, при этом перечисление источников осуществляется в алфавитном порядке или в соответствии с хронологическим принципом. Список оформляется в соответствии с требованиями: ГОСТ 7.1-2003 «Библиографическая запись. Библиографическое описание. Общие требования и правила составления»; ГОСТ 7.12-77 «Сокращение русских слов и словосочетаний в библиографическом описании»; ГОСТ 7.11-78 «Сокращение слов и словосочетаний на иностранных языках в библиографическом описании»; ГОСТ 7.80-2000 «Библиографическая запись. Заголовок. Общие требования и правила составления».

В приложения могут быть вынесены рисунки, таблицы, графики, диаграммы, иллюстрации, программные коды.

К ВКР предъявляются следующие требования:

- соответствие название ВКР направлению подготовки 10.05.01 Компьютерная безопасность, видам профессиональной деятельности, направленности программы специалитета;
- актуальность темы исследования, соответствие современному состоянию предметной области;
- четкая логическая структура, обусловленная последовательностью решения задач для достижения цели исследования;
- корректное изложение с учетом принятой научной терминологии;
- оформление в соответствии с требованиями стандартов ЕСКД, ЕСТД и ЕСПД, а также стандарта ГОСТ 7.32-91 (ИСО 5966-82) «Отчет о научно-исследовательской работе. Структура и правила оформления».

Текст ВКР должен быть выполнен печатным способом на одной стороне листа белой бумаги формата А4 (297×210 мм). Для основного текста рекомендуется шрифт Times New Roman 14 размера, полуторный интервал. Поля: верхнее – 2 см, нижнее – 2 см; левое – 3 см (для переплета), правое – 1 см. Нумерация страниц – сквозная, номер страницы проставляется арабскими цифрами в центре листа внизу страницы. Титульный лист не нумеруется. Допускается оформлять иллюстрации и таблицы на листах формата А3 (297×420 мм).

Рекомендованный объем ВКР составляет от 45 до 70 страниц через полуторный интервал, не включая приложений.

Ответственность за правильность оформления ВКР и верность приведенных в ней результатов (в том числе цитируемых) несет обучающийся.

13.4. Результаты обучения, характеризующие готовность выпускника к профессиональной деятельности, проверяемые на защите ВКР:

Коды компетенций (общекультурных, общепрофессиональных, профессиональных, дополнительных)	Результаты обучения	Примечание
ОК-5	<p>Знать: методы исследования и оценивания объектов информатизации с точки зрения обеспечения информационной защиты; 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.</p> <p>Уметь: работать в коллективе; решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом требований информационной безопасности; принимать участие в формировании, организации и поддержке выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации.</p> <p>Владеть: навыками публичного представления собственных и известных научных результатов.</p>	

ОК-7	<p>Знать: иностранный язык в объеме, необходимом для получения профессиональной информации из зарубежных источников и общения на деловом уровне; профессиональную лексику иностранного языка в объеме, необходимом для общения, чтения и перевода иноязычных текстов в рамках делового общения в профессиональной деятельности; основные грамматические явления и структуры государственного (русского) языка, используемые в устном и письменном общении в профессиональной деятельности.</p> <p>Уметь: использовать иностранный язык в межличностном общении и профессиональной деятельности; соблюдать речевой этикет в ситуациях повседневного и делового общения (устанавливать и поддерживать контакты, завершить беседу, запрашивать и сообщать информацию).</p> <p>Владеть: основами публичной речи, перевода текстов по специальности; навыками грамотно и эффективно пользоваться источниками информации (справочной литературой, ресурсами Интернет); навыками выражения своего мнения в процессе делового общения на иностранном языке.</p>	
ОПК-2	<p>Знать основные понятия и методы математического анализа, аналитической геометрии, линейной алгебры, теории комплексного переменного.</p> <p>Уметь применять математические методы и модели для решения прикладных задач профессиональной области.</p> <p>Владеть навыками применения математического аппарата для анализа процессов обработки, поиска и передачи информации в экспериментальных исследованиях при решении прикладных задач профессиональной области.</p>	
ОПК-3	<p>Знать определение информации и ее роль в развитии общества.</p> <p>Уметь применять современные информационные технологии для поиска и обработки информации по профилю деятельности в глобальных компьютерных системах, сетях, в библиотечных фондах и в иных источниках информации.</p> <p>Владеть навыками поиска и автоматизированной обработки информации.</p>	
ОПК-4	<p>Знать основные методы обобщения, восприятия и анализа информации при решении профессиональных задач.</p> <p>Уметь формулировать результат проведенных исследований в виде конкретных рекомендаций, выраженных в терминах предметной области при решении профессиональных задач.</p> <p>Владеть навыками применения современных методов научных исследований при решении профессиональных задач.</p>	
ОПК-5	<p>Знать: правовые основы обеспечения информационной безопасности.</p> <p>Уметь: применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности.</p> <p>Владеть: навыками работы с нормативными правовыми актами.</p>	

ОПК-7	<p>Знать: принципы организации информационных систем в соответствии с требованиями по защите информации.</p> <p>Уметь: осуществлять меры противодействия нарушениям информационной безопасности.</p> <p>Владеть: профессиональной терминологией, навыками использования программных средств системного, прикладного и специального назначения.</p>	
ОПК-8	<p>Знать: Основы разработки Enterprise-приложений на платформе J2EE</p> <p>Уметь: использовать платформу J2EE для решения профессиональных, исследовательских и прикладных задач, логически мыслить, самостоятельно расширять свои знания по разработке Enterprise-приложений</p> <p>Владеть: методами проектирования Enterprise-приложений</p>	
ОПК-10	<p>Знать: основные угрозы безопасности информации и модели нарушителя в информационных системах.</p> <p>Уметь: определять комплекс мер для обеспечения информационной безопасности информационных систем.</p> <p>Владеть: навыками формальной постановки и решения задачи обеспечения информационной безопасности, навыками анализа информационной инфраструктуры информационной системы и ее безопасности.</p>	
ПК-1	<p>Знать основы организационного и правового обеспечения в области информационной безопасности и защиты информации.</p> <p>Уметь пользоваться нормативными документами и методиками проверки защищенности объекта информатизации.</p> <p>Владеть навыками работы с нормативными правовыми актами в области ИБ.</p>	
ПСК-2.1	<p>Знать принципы и методы построения быстрых алгоритмов для реализации систем защиты информации.</p> <p>Уметь разрабатывать быстрые вычислительные алгоритмы для криптографических приложений.</p> <p>Владеть методами построения быстрых вычислительных алгоритмов для решения профессиональных задач.</p>	
ПСК-2.4	<p>Знание видов UNIX-систем, представление об архитектуре UNIX-систем.</p> <p>Умение производить настройку UNIX-системы, назначать права пользователям, производить удаленное администрирование системы.</p> <p>Владение техникой администрирования UNIX-систем и навыками настройки системы безопасности. UNIX-систем, представление об архитектуре UNIX-систем.</p>	

13.5 Процедура защиты ВКР и методические рекомендации для студента

Защита ВКР проводится в соответствии с Положением о порядке проведения государственной итоговой аттестации по образовательным программам высшего образования – программам бакалавриата, программам специалитета и программам магистратуры воронежского государственного университета П ВГУ 2.1.28 – 2018.

К защите ВКР допускается обучающийся, успешно завершивший в полном объеме освоение основной образовательной программы по данному направлению и полностью выполнивший задание на выполнение ВКР. Готовность ВКР к защите определяется решением заседания кафедры на основании проведенной (не позднее, чем за 2 недели до защиты) предзащиты и проверки на объем заимствования. Допуск к защите фиксируется

подписью заведующего кафедрой на титульном листе.

При представлении ВКР к защите должны быть соблюдены следующие требования:

- объем заимствования составляет не более 35 %;
- обучающимся получены отзывы научного руководителя;
- на титульном листе ВКР имеются подписи обучающегося, научного руководителя, консультанта (при наличии), заведующего кафедрой;
- ВКР размещена на образовательном портале «Электронный университет».

В ГЭК обучающимся предоставляются следующие документы: зачетная книжка с соответствующей отметкой о допуске к ГИА, ВКР и ее электронная копия, отзыв научного руководителя, рецензия.

Защита ВКР является публичной и проходит на открытом заседании ГЭК с участием не менее двух третей ее состава и председателя ГЭК. В исключительных случаях председатель может поручить свои функции одному из членов ГЭК.

Присутствие научного руководителя ВКР и рецензента (или хотя бы одного из них) является обязательным, их отзывы зачитываются председателем.

Процедура защиты включает следующие этапы:

- представление обучающегося, оглашение темы ВКР;
- доклад обучающегося (10-15 минут с акцентом на собственные результаты и полученные выводы);
- вопросы обучающемуся со стороны членов комиссии и присутствующих на защите;
- выступление научного руководителя (или председателем зачитывается отзыв);
- выступление рецензента (или председателем зачитывается отзыв);
- дискуссия;
- заключительное слово обучающегося.

По окончании всех запланированных на данное заседание защит ГЭК проводит закрытое совещание, на котором каждому обучающемуся выставляется оценка в шкале {отлично, хорошо, удовлетворительно, неудовлетворительно}. Процедура обсуждения устанавливается председателем ГЭК. В спорных случаях решение выносится простым большинством голосов членов ГЭК, а при равенстве голосов решающим является голос председателя. Решение по каждой ВКР фиксируется в оценочном листе ВКР.

Результаты защиты ВКР с возможными рекомендациями (в аспирантуру, к внедрению, к опубликованию) объявляются обучающимся в тот же день после оформления протоколов заседания ГЭК в установленном порядке и вносятся в зачетные книжки и ведомости. Оценка «неудовлетворительно» вносится только в ведомость.

Подача и рассмотрение апелляционных заявлений по результатам ИГА регламентируются «Положением о порядке проведения государственной итоговой аттестации по образовательным программам высшего образования – программам бакалавриата, программам специалитета и программам магистратуры воронежского государственного университета П ВГУ 2.1.28 – 2018».

В случае успешной защиты ВКР обучающийся получает степень Специалиста по защите информации.

ВКР хранится на выпускающей кафедре в течении 5 лет.

13.6. Фонд оценочных средств для защиты ВКР

13.6.1. Примерный перечень вопросов на защите ВКР

1. Поясните, чем обеспечивается в Вашей работе отказоустойчивой модели информационной платформы?
2. Что позволяет говорить в 2 классе отказоустойчивости Вашей модели центра обработки данных?

3. Поясните практическую необходимость Вашего клиент-серверного решения аудита?
4. Чем обоснован выбор ПО для аналитической обработки информации в режиме реального времени?
5. Для каких ERP-систем Ваши модели и решения информационной безопасности применимы?
6. Какие перспективы повышения защищенности, разработанной Вами модели Вы видите?
7. Зачем проводить дополнительное моделирование отказоустойчивости и переполнения сервера базы данных если современные СУБД имеют инструменты балансировки нагрузки?
8. Какие методы моделирования пропускной способности с Вашей точки зрения наиболее применимы для корпоративных сетей, и почему?
9. Какова практическая значимость и применимость разработанных алгоритма и программы постквантовой криптографии?
10. Чем подтверждается эффективность Ваши средства математического обеспечения информационных систем?

13.6.2. Критерии и шкала оценивания результатов ВКР

Критериями оценки ВКР по направлению подготовки 10.05.01 Компьютерная безопасность (специалист), являются:

- компетентность в исследуемой предметной области;
- качество постановки задачи;
- обоснование выбора и/или знание метода решения задачи;
- качество изложения материала ВКР;
- уровень программной реализации (при условии, что она является неотъемлемой частью ВКР);
- представление результатов исследования (раздаточный материал, презентация);
- ответы на вопросы;
- оценка руководителя;
- оценка рецензента;
- наличие публикаций и/или внедрений.

В процессе оценивания по каждому критерию выставляется соответствующий балл (Таблица 1).

Таблица 1 – Шкалы критериев оценки ВКР

№	Критерий	Баллы	Признаки
1	Компетентность в предметной области	3	Обучающийся хорошо ориентируется в предметной области.
		2	Знание предметной области является неполным.
		1	Обучающийся неуверенно владеет терминологией предметной области.
2	Качество постановки задачи	3	Содержательная постановка задачи сформулирована четко, грамотно произведен переход к формальной постановке задачи.
		2	Постановка задачи сформулирована нечетко.
		1	Содержательная постановка задачи сформулирована нечетко, имеются погрешности при формализации.

3	Обоснование выбора и/или знание метода решения задачи	8	Выбор метода полностью обоснован и/или обучающийся продемонстрировал глубокое знание метода решения задачи. Реализация метода осуществлена качественно.
		4	Выбор метода обоснован недостаточно и/или обучающийся не в полной мере владеет методом. Реализация метода осуществлена в соответствии с техникой владения.
		1	Выбор метода не обоснован и/или имеются ошибки в описании и реализации метода решения задачи.
4	Качество изложения материала	3	Материал изложен логично, используемая терминология соответствует предметной области, список использованных источников содержит современные публикации, при решении практических задач используются данные за последние 5 лет, ВКР оформлена в соответствии с требованиями.
		2	Используемая терминология отличается нечеткостью формулировок, теоретическая база не содержит ссылки на современные публикации, ВКР оформлена в соответствии с требованиями.
		1	Изложение материала в основном верное, но содержит ошибочные утверждения, нарушены существенные требования к оформлению ВКР.
5	Уровень программной реализации		
5.1	Интерфейс	2	Наглядный вывод запросов к пользователю, полнота запросов, удобное и полное представление данных.
		1	Набор запросов неполный, в выводе результатов имеются неточности.
		0	Неполный набор запросов, неполный вывод результатов.
5.2	Структурированность программы и наличие комментариев	2	Программа структурирована, комментариев достаточно.
		1	Программа структурирована, комментариев недостаточно.
		0	Программа не структурирована, комментарии отсутствуют.
5.3	Освоение среды разработки и выполнения программы	2	Основные возможности среды освоены.
		1	Основные возможности среды освоены частично.
		0	Допущены ошибки при работе в среде.
6	Представление результатов исследования (раздаточный	2	Раздаточный материал и/или презентация дают полное представление о

	материал, презентация)		результатах проведенного исследования и соответствуют содержанию работы, качественно оформлены.
		1	Раздаточный материал и/или презентация не полно отражают основное содержание работы, имеются погрешности в оформлении.
		0	Раздаточный материал и/или презентация не отражают суть работы и полученных результатов.
7	Ответы на вопросы	3	Ответы на вопросы полные и обоснованные.
		2	Неполные ответы на вопросы.
		1	Ответы содержат ошибки и неточности.
		0	Неверные ответы на вопросы или ответы отсутствуют.
8	Оценка руководителя	5, 4, 3, 0	
9	Оценка рецензента	5, 4, 3, 0	
10	Наличие публикаций и/или внедрений	1+1	Имеется публикация и/или внедрение.
		0	Публикация и внедрение отсутствуют.

Уровень программной реализации учитывается при условии, что она, по мнению руководителя, является неотъемлемой частью ВКР.

Для оценивания результатов защиты выпускной квалификационной работы может использоваться шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Критерии и шкала оценивания ВКР представлены в таблице:

Шкала оценок	Критерии оценивания
Отлично	Грамотно и четко сформулирована постановка задачи, продемонстрирован высокий уровень готовности использовать навыки выбора, проектирования, реализации, оценки качества и анализа эффективности программного обеспечения для решения задач в различных предметных областях, продемонстрирован высокий уровень готовности к использованию основных моделей информационных технологий и способов их применения для решения задач в предметных областях, выявлена ярко выраженная способность к самоорганизации и самообразованию, четко и качественно изложен материал работы, четко и квалифицированно даны ответы на все дополнительные вопросы, отзыв носит положительный характер

Хорошо	Корректно сформулирована постановка задачи, продемонстрирована готовность использовать навыки выбора, проектирования, реализации, оценки качества и анализа эффективности программного обеспечения для решения задач в различных предметных областях, продемонстрирована готовность к использованию основных моделей информационных технологий и способов их применения для решения задач в предметных областях, выявлена способность к самоорганизации и самообразованию, четко и качественно изложен материал работы, не на все дополнительные вопросы даны исчерпывающие ответы, имеются претензии к объему выполненной работы, отзыв носит положительный характер
Удовлетворительно	Компетентность в предметной области продемонстрирована недостаточно, постановка задачи сформулирована расплывчато, недостаточно четко продемонстрирована готовность использовать навыки выбора, проектирования, реализации, оценки качества и анализа эффективности программного обеспечения для решения задач в различных предметных областях, выявлены незначительные пробелы в готовности к использованию основных моделей информационных технологий и способов их применения для решения задач в предметных областях, выявлен невысокий уровень способностей к самоорганизации и самообразованию, изложение материала работы содержит нечеткие формулировки и является непоследовательным, ответы на дополнительные вопросы неполные или содержат неточности и ошибочные утверждения, дан положительный отзыв
Неудовлетворительно	Низкий уровень компетентности в предметной области, постановка задачи сформулирована нечетко и с погрешностями, низкий уровень теоретической и практической подготовки, недостаточное владение или неиспользование современных информационных технологий, изложение материала работы содержит нечеткие формулировки и ошибочные утверждения, даны неверные ответы на дополнительные вопросы

13.6.3. Методические материалы, определяющие процедуры оценивания:

По всем критериям каждый член ГЭК выставляет баллы, которые в дальнейшем суммируются.

Подведение итогов: Оценка ВКР формируется с учетом баллов, полученных по критериям. Шкала оценок представлена в табл. 2.

Таблица 2 – Шкала оценок ВКР

Оценка ВКР	Программная реализация предусмотрена	Программная реализация не предусмотрена
Отлично	не менее 29	не менее 23
Хорошо	не менее 21 не более 28	не менее 18 не более 22
Удовлетворительно	не менее 12 не более 20	не менее 10 не более 17
Неудовлетворительно	менее 12	менее 10

Итоговая оценка определяется как средняя арифметическая всех индивидуальных оценок членов ГЭК.

В спорных случаях решение выносится простым большинством голосов членов ГЭК, а при равенстве голосов решающим является голос председателя.

13.7. Перечень учебной литературы, ресурсов сети «Интернет», необходимых для подготовки к защите и процедуры защиты ВКР

а) основная литература:

№ п/п	Источник
1	Шкляр, М.Ф. Основы научных исследований / М.Ф. Шкляр. — Москва: Дашков и Ко, 2012. — 244 с. URL: http://biblioclub.ru/index.php?page=book&id=112247 .
2	Новиков А.М., Новиков Д.А. Методология научного исследования. – М.: Либроком. 2010 – 280 с. URL: http://www.methodolog.ru/books/mni.pdf .
3	Фостер, Джеймс. Защита от взлома: сокетты, эксплойты, shell-код: / Дж. Фостер, М. Прайс ; пер. с англ. А. А. Слинкина .— Москва : ДМК Пресс, 2008 .— 784 с. : ил. — (Информационная безопасность).— ISBN 5-9706-0019-9 : 449.10 р. — <URL: http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1117 >.
4	Скудис, Эд. Противостояние хакерам. Пошаговое руководство по компьютерным атакам и эффективной защите/ Э. Скудис. — Москва: ДМК Пресс, 2009. — 512 с. : ил. — (Защита и администрирование) .— ISBN 5-94074-170-3 : 176-00 .— <URL: http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1112 >.
5	Голуб, Владимир Александрович. Защита от вредоносного программного обеспечения: учебное пособие для вузов / В.А. Голуб; Воронеж. гос. ун-т.— Воронеж: ЛОП ВГУ, 2006. — 31 с. — Библиогр.: с.30 .— <URL: http://www.lib.vsu.ru/elib/texts/method/vsu/may07045.pdf >.
6	Ховард, Майкл. 19 смертных грехов, угрожающих безопасности программ. Как не допустить типичных ошибок/ М. Ховард, Д. Лебланк, Дж. Виега; авт. предисл. А. Йоран. — Москва: ДМК Пресс, 2009. — 287 с. : ил. — .— Загл. и авт. ориг.: 19 deadly sins of software security / Michael Howard, David Leblanc, John Viega .— ISBN 5-9706-0027-X .— <URL: http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1118 >.
7	Управление внедрением информационных систем: курс лекций: учеб. пособие для студентов вузов, обучающихся по специальностям в области информ. технологий / В.И. Грекул, Г. Н. Денищенко, Н.Л. Коровкина. – М.: Интернет-Ун-т информ. технологий, 2008. [Электронный ресурс] URL: http://www.intuit.ru/studies/courses/2196/267/info/ .
8	Юрин И.Ю. Теоретические и практические основы защиты информации. 2012. http://library.sgu.ru/uch_lit/620.pdf .

б) дополнительная литература:

№ п/п	Источник
9	Кручинин, В.В. <i>Компьютерные технологии</i> в научных исследованиях: учебно-методическое пособие / В.В. Кручинин. – Москва: ТУСУР (Томский государственный университет систем управления и радиоэлектроники), 2012. — 57 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=11269 .
10	Андреев, Г.И. Основы научной работы и методология диссертационного исследования / Г.И. Андреев, В.В. Барвиненко, В.С. Верба. — Москва: Финансы и статистика, 2012. — 296 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=28348 .
11	Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации, 31.07.2006, № 31 (1 ч.), ст. 3448.
12	Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» // Собрание законодательства Российской Федерации, 31 июля 2006 года № 31 (1 ч.), ст. 3451.
13	ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. (утверждён и введён в действие Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 375-ст).
14	Приказ Федеральной службы по техническому и экспортному контролю России от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» // Российская газета, № 136, 26.06.2013.
15	Приказ Федеральной службы по техническому и экспортному контролю России от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по

	обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» // Российская газета, № 107, 22.05.2013.
16	Методический документ. Меры защиты информации в государственных информационных системах (утв. ФСТЭК России 11.02.2014).
17	Постановление Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // Собрание законодательства Российской Федерации, 05.11.2012, № 45, ст. 6257.
18	Постановление правительства Воронежской области от 28 апреля 2011 года № 340 «Об утверждении положения о едином реестре государственных информационных систем Воронежской области» // Собрание законодательства Воронежской области 20.06.2011 № 4, ст. 285.
19	Александр Доронин. Бизнес-разведка http://fxt.com.ua/business_literatura/131-aleksandr-doronin-biznes-razvedka.html .
20	ГОСТ Р ИСО/МЭК 15408-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий», принят и введен в действие Постановлением Госстандарта России от 4 апреля 2002 г. № 133-ст.
21	ИСО/МЭК 31000:2009 «Управление рисками. Принципы и направления», ISO Technical Management Board Working Group, 2009.
22	ИСО/МЭК 31100:2009 «Управление рисками. Методики оценки риска», ISO Technical Management Board Working Group, 2009.
23	ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения информационной безопасности. Менеджмент риска информационной безопасности», утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 30 ноября 2010 г. № 632-ст.

в) информационные электронно-образовательные ресурсы (официальные ресурсы интернет)

№ п/п	Ресурс
24	Электронная библиотека рабочих учебных программ дисциплин. Режим доступа: http://smwww.main.vsu.ru
25	Электронная библиотека учебно-методических материалов ВГУ. Режим доступа: http://www.lib.vsu.ru
26	Портал государственных услуг Российской Федерации www.gosuslugi.ru
27	http://www.cryptopro.ru
28	http://www.infotecs.ru
29	Фундаментальные и прикладные исследования в области параллельных вычислений. Режим доступа http://parallel.ru/research свободный
30	http://www.lissi-crypto.ru/
31	http://www.signal-com.ru
32	http://www.shipka.ru

Обучающийся дополнительно использует литературу, соответствующую тематике ВКР.

13.8. Информационные технологии, используемые для подготовки к защите и процедуры защиты ВКР, включая программное обеспечение и информационно-справочные системы

ОС Windows, PowerPoint, PDF reader и программное обеспечение необходимое для демонстрации разработанных в ходе ВКР программных решений. Подключение к сети Internet для демонстрации практической составляющей ВКР ориентированных на построение сайтов или использование технологий Internet.

13.9. Материально-техническое обеспечение:

Материально-техническое обеспечение государственной итоговой аттестации предусматривает наличие аудитории для защиты выпускной квалификационной работы.

Для защиты выпускной квалификационной работы требуется аудитория, предусматривающая наличие рабочих мест для председателя и членов государственной экзаменационной комиссии, рабочего места для студента, компьютерной техники с необходимым лицензионным программным обеспечением, мультимедийного проектора, экрана.