

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

Декан факультета прикладной математики,  
информатики и механики  
Шашкин А.И.  
24.06.2021 г.



**ПРОГРАММА  
ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ**

**1. Код и наименование направления подготовки:**

10.05.01 Компьютерная безопасность

**2. Профиль подготовки:**

Математические методы защиты информации

**3. Квалификация выпускника:** Специалист

**4. Форма(ы) обучения:** очная

**5. Утверждена** Ученым советом факультета прикладной математики, информатики и механики (протокол № 10 от 15.06.2021)

**6. Учебный год:** 2026/2027

**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 26.11.2020 № 1459.

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

**9. Форма(ы) государственной итоговой аттестации:**

Подготовка к процедуре защиты и защита выпускной квалификационной работы (ВКР).

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

| Код                                     | Название  |
|---|---|
| <b>Универсальные компетенции</b>        |   |
| УК-1                                    | Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, выработать стратегию действий  |
| УК-2                                    | Способен управлять проектом на всех этапах его жизненного цикла   |
| УК-4                                    | Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия  |
| <b>Общепрофессиональные компетенции</b> |   |
| ОПК-2                                   | Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности;  |
| ОПК-3                                   | Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности;  |
| ОПК-5                                   | Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;   |
| ОПК-6                                   | Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю; |
| ОПК-7                                   | Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ;  |
| ОПК-8                                   | Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей;  |
| ОПК-9                                   | Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации;          |
| ОПК-10                                  | Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности;   |
| ОПК-11                                  | Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации;   |
| ОПК-12                                  | Способен администрировать операционные системы и выполнять работы по  |

|                                     |   |
|-------------------------------------|---|
|                                     | восстановлению работоспособности прикладного и системного программного обеспечения;   |
| ОПК-13                              | Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности;   |
| ОПК-14                              | Способен проектировать базы данных, администрировать системы управления базами данных в соответствии с требованиями по защите информации;   |
| ОПК-15                              | Способен администрировать компьютерные сети и контролировать корректность их функционирования;  |
| ОПК-16                              | Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях;   |
| ОПК-2.1                             | Способен разрабатывать алгоритмы, реализующие современные математические методы защиты информации   |
| ОПК-2.2                             | Способен разрабатывать и анализировать математические модели механизмов защиты информации   |
| ОПК-2.3                             | Способен проводить сравнительный анализ и осуществлять обоснованный выбор программных и программно-аппаратных средств защиты информации с учетом реализованных в них математических методов   |
| <b>Профессиональные компетенции</b> |   |
| ПК-1                                | Способен проводить анализ требований и выполнять работы по проектированию программного обеспечения с применением математических методов защиты  |
| ПК-2                                | Способен проводить исследования на всех этапах жизненного цикла средств защиты информации в профессиональной деятельности   |
| ПК-3                                | Способен осуществлять разработку, анализ и обосновывать эффективность применяемых математических методов защиты информации, возникающих при работе программных и программно-аппаратных средств защиты информации при решении профессиональных, исследовательских и прикладных задач |

**11. Объем государственной итоговой аттестации в зачетных единицах / ак. час. – 6 / 216.**

подготовка к защите и процедура защиты ВКР – 6 / 216.

## **12 Требования к ВКР**

### **12.1 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 ОПОП в соответствии с учебным планом, полностью выполнивший задание кафедры на выполнение ВКР.

Темы квалификационная 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 квалификационная работ разрабатывается преподавателями выпускающей кафедры. Примерная тематика квалификационная 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 ВКР.

## **12.2 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 распределенных 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.

## **12.3 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.

#### Требования к структуре ВКР:

Титульный лист должен быть оформлен в соответствии с СТП ВГУ.

Содержание включает наименования всех разделов, подразделов (глав, параграфов), пунктов (если они имеются) с указанием номеров страниц, на которых размещается начало материала раздела, подраздела, главы, параграфа, пункта. Во введении обосновывается выбор темы, определяемый ее актуальностью, формулируются проблема и круг вопросов, необходимых для ее решения; определяется цель работы с ее расчленением на взаимосвязанный комплекс задач, подлежащих решению, для раскрытия темы; указываются объект исследования, используемые методы анализа и литературные источники; определяется структура работы.

В основной части раскрывается содержание выпускной квалификационной работы.

Первая глава носит, как правило, общетеоретический (методологический) характер. В ней на основе изучения работ отечественных и зарубежных авторов излагается актуальность и сущность исследуемой проблемы, рассматриваются различные подходы к решению, дается их оценка, обосновываются и излагаются собственные позиции студента. Эта глава служит теоретическим обоснованием исследований, проведенных студентом.

Обоснование цели ВКР необходимо проводить на основе анализа современного состояния и тенденций развития проблемы.

Во второй главе приводится постановка задачи, ее содержательное и математическое описание. Для ВКР, связанных с разработкой информационных систем и использованием информационных технологий, в содержательной постановке приводятся ссылки на документы, регламентирующие процесс функционирования информационной системы; основные показатели, которые должны быть достигнуты в условиях эксплуатации информационной системы; ограничения на время решения поставленной задачи; сроки выдачи информации; способы организации диалога человека с информационной системой средствами имеющегося инструментария, описание входной и выходной информации (форма представления сообщений, описание структурных единиц, периодичность выдачи информации или частота поступления), требования к организации сбора и передачи входной информации, ее контроль и корректировка.

В математической постановке выполняется формализация задачи, в результате которой определяется состав переменных, констант и их классификация, виды ограничений на переменные и математические зависимости между переменными. Устанавливается класс, к которому относится решаемая задача, и приводится сравнительный анализ методов решения для выбора наиболее эффективного метода. Приводится обоснование принятых допущений и предпосылок при формализации и выборе метода решения. Определяется общая последовательность решения задачи.

В этой же главе приводятся результаты теоретических исследований, описание разработанных алгоритмов, анализ их эффективности.

Для ВКР, связанных с разработкой информационных систем и использованием информационных технологий, необходимо уделить внимание вопросам организации баз данных и баз знаний, требованиям к организации сбора, передачи и контроля информации.

Обоснование выбора или разработки технического обеспечения информационной системы основывается на принципах организации и функционирования ЭВМ, систем, комплексов, использовании локальных и глобальных вычислительных сетей.

Программное обеспечение должно включать структуру программно-методического комплекса, функции программ структурных уровней, способы реализации монитора управления нижними уровнями программных модулей, способы реализации модулей ввода и вывода информации.

Если ВКР посвящена решению конкретной прикладной задачи, то результаты вычислительного эксперимента и/или анализ решения задачи целесообразно выделить в отдельную главу (раздел).

Тексты программ оформляются в виде отдельного документа и помещаются в приложение.

Обязательными для ВКР являются логическая связь между главами и последовательное развитие основной темы на протяжении всей работы.

В заключении логически последовательно излагаются теоретические и практические выводы и предложения, к которым пришел студент в результате исследования. Они должны быть краткими, четкими, дающими полное представление о содержании, значимости, обоснованности и эффективности разработок.

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 следует поместить вспомогательный материал, который при включении в основную часть работы загромождает текст. К нему можно отнести: промежуточные теоретические выкладки и расчеты, некоторые доказательства, таблицы данных, текст программы, иллюстрации вспомогательного характера.

Приложения располагаются в порядке появления ссылок на них в основном тексте работы. Количество приложений в работе определяется только необходимостью их введения в работу. При оформлении приложения указывается не только его номер, но и название приложения, отражающего его суть. В качестве образца оформления приложений можно воспользоваться приложениями данного методического пособия.

К ВКР предъявляются следующие требования:

- соответствие названию 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.

#### 12.4 Результаты обучения, характеризующие готовность выпускника к профессиональной деятельности, проверяемые на защите ВКР:

| Коды компетенций | Код и наименование индикаторов достижения компетенции  |
|------------------|--|
| УК-1             | УК-1.1 Определяет пробелы в информации, необходимой для решения проблемной ситуации.<br>УК-1.2 Критически оценивает надежность источников информации, работает с противоречивой информацией из разных источников.<br>УК-1.3 Рассматривает возможные варианты решения задачи, оценивая достоинства и недостатки.  |
| УК-2             | УК-2.1 Формулирует конкретную, специфичную, измеримую во времени и пространстве цель, а также определяет дорожную карту движения к цели, исходя из имеющихся ресурсов и ограничений.<br>УК-2.2 Проектирует решение конкретной задачи с учетом возможных ограничений действующих правовых норм. Составляет иерархическую структуру работ, распределяет по задачам финансовые и трудовые ресурсы, использует актуальное ПО.  |
| УК-4             | УК-4.2 Владеет культурой письменного и устного оформления профессионально ориентированного научного текста на государственном языке РФ.  |
| ОПК-2            | ОПК-2.6 Умеет составлять документы, используя прикладные программы офисного назначения.<br>ОПК-2.7 владеет средствами управления пользователями интерфейсами операционных систем.<br>ОПК-2.8 знает основные принципы конфигурирования и администрирования операционных систем.<br>ОПК-2.9 умеет разрабатывать системное и прикладное программное обеспечение для многозадачных, многопользовательских и многопроцессорных сред, а также для сред с интерфейсом, управляемым сообщениями.<br>ОПК-2.10 умеет применять основные методы программирования в выбранной операционной среде.<br>ОПК-2.11 Знает характерные особенности современного программного обеспечения специального назначения.<br>ОПК-2.12 Умеет производить установку, наладку, тестирование и обслуживание программного обеспечения, включая решения отечественного производства.<br>ОПК-2.13 Умеет производить установку, наладку, тестирование и обслуживание сетевого программного обеспечения, включая решения отечественного производства.<br>ОПК-2.14 Умеет производить установку, наладку, тестирование и обслуживание современных программных средств обеспечения информационной безопасности. |
| ОПК-3            | ОПК-3.13 умеет производить оценку качества полученных решений прикладных задач.<br>ОПК-3.20 знает различные подходы к определению понятия алгоритма, методы доказательства алгоритмической неразрешимости и методы построения эффективных алгоритмов.<br>ОПК-3.23 умеет оценивать сложность алгоритмов и вычислений.<br>ОПК-3.35 умеет применять стандартные методы дискретной математики для решения профессиональных задач.<br>ОПК-3.37 владеет навыками применения языка и средств дискретной математики при решении профессиональных задач.<br>ОПК-3.57 умеет разрабатывать и использовать вероятностные и статистические модели при решении типовых прикладных задач.   |

|        |  |
|--------|--|
| ОПК-5  | <p>ОПК-5.3 умеет классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности.</p> <p>ОПК-5.4 умеет классифицировать и оценивать угрозы информационной безопасности для объекта информатизации.</p> <p>ОПК-5.8 знает правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности.</p> <p>ОПК-5.19 владеет методами и средствами технической защиты информации.</p>  |
| ОПК-6  | <p>ОПК-6.5 знает основные угрозы безопасности информации и модели нарушителя компьютерных систем.</p> <p>ОПК-6.8 умеет определить политику контроля доступа работников к информации ограниченного доступа.</p>   |
| ОПК-7  | <p>ОПК-7.4 умеет работать с интегрированной средой разработки программного обеспечения.</p> <p>ОПК-7.5 умеет разрабатывать и реализовывать на языке высокого уровня алгоритмы решения типовых профессиональных задач.</p> <p>ОПК-7.6 владеет навыками разработки, документирования, тестирования и отладки программ.</p> <p>ОПК-7.10 умеет применять известные методы программирования и возможности базового языка программирования для решения типовых профессиональных задач.</p> <p>ОПК-7.11 владеет навыками разработки алгоритмов решения типовых профессиональных задач.</p> <p>ОПК-7.12 Знает необходимые и достаточные условия оптимальности задачи математического программирования.</p> <p>ОПК-7.13 Умеет применять методы одномерной оптимизации при решении прикладных задач.</p> <p>ОПК-7.14 Умеет использовать методы многомерной безусловной оптимизации при решении профессиональных задач.</p> <p>ОПК-7.15 Знает методы условной оптимизации при решении прикладных задач.</p> |
| ОПК-8  | <p>ОПК-8.10 умеет разрабатывать модели безопасности компьютерных систем с использованием необходимого математического аппарата и средств компьютерного моделирования.</p> <p>ОПК-8.11 владеет способами моделирования безопасности компьютерных систем, в том числе моделирования управления доступом и информационными потоками в компьютерных системах.</p> <p>ОПК-8.12 Знает современные методы обработки информации и машинного обучения.</p> <p>ОПК-8.13 Умеет применять методы машинного обучения при проведении разработок в области обеспечения безопасности компьютерных систем.</p> <p>ОПК-8.14 знает методологию экспериментальных исследований и испытаний.</p> <p>ОПК-8.15 умеет применять методы экспериментального исследования при решении профессиональных задач.</p>   |
| ОПК-9  | <p>ОПК-9.9 умеет формулировать и настраивать политику безопасности локальных компьютерных сетей, построенных на основе основных операционных систем.</p> <p>ОПК-9.10 знает общие и специфические угрозы безопасности баз данных.</p> <p>ОПК-9.11 Знает основные тенденции развития методов защиты информации в операционных системах и системах управления базами данных.</p> <p>ОПК-9.12 знает общие и специфические угрозы безопасности операционных систем и систем управления баз данных.</p> <p>ОПК-9.16 владеет методами и средствами технической защиты информации.</p>   |
| ОПК-10 | <p>ОПК-10.4 умеет корректно использовать криптографические алгоритмы на практике при решении задач криптографическими методами.</p> <p>ОПК-10.5 умеет применять математические методы при исследовании криптографических алгоритмов.</p> <p>ОПК-10.10 умеет проводить анализ криптографических протоколов, в том числе с использованием автоматизированных средств.</p> <p>ОПК-10.26 умеет решать типовые задачи кодирования и декодирования.</p> <p>ОПК-10.28 владеет навыками применения математического аппарата для решения прикладных теоретико-информационных задач.</p>   |
| ОПК-11 | <p>ОПК-11.1 знает основные понятия и определения, используемые при описании моделей безопасности компьютерных систем.</p> <p>ОПК-11.2 знает основные виды политик управления доступом и информационными потоками в компьютерных системах.</p> <p>ОПК-11.3 знает основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков.</p> <p>ОПК-11.5 умеет разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками.</p> <p>ОПК-11.10 умеет формулировать и настраивать политику безопасности локальных компьютерных сетей, построенных на базе основных операционных систем.</p>  |
| ОПК-12 | <p>ОПК-12.4 владеет навыками системного программирования.</p> <p>ОПК-12.5 Умеет осуществлять администрирование программного обеспечения специального назначения, включая операционные системы, в том числе отечественного производства.</p>  |



|         |   |
|---------|---|
| ОПК-13  | <p>ОПК-13.12 умеет формализовать поставленную задачу.</p> <p>ОПК-13.13 умеет разрабатывать эффективные алгоритмы и программы.</p> <p>ОПК-13.14 умеет проводить оценку вычислительной сложности алгоритма.</p> <p>ОПК-13.15 умеет планировать разработку сложного программного обеспечения.</p> <p>ОПК-13.16 владеет методами оценки качества готового программного обеспечения.</p> <p>ОПК-13.17 владеет навыками разработки алгоритмов для решения типовых профессиональных задач.</p>   |
| ОПК-14  | ОПК-14.14 владеет методикой и навыками использования средств защиты, предоставляемых СУБД.  |
| ОПК-15  | <p>ОПК-15.2 знает основы организации и построения компьютерных сетей.</p> <p>ОПК-15.5 умеет реализовывать приложения для сетевых интерфейсов на нескольких современных программно-аппаратных платформах.</p> <p>ОПК-15.7 владеет навыками администрирования компьютерных сетей.</p> <p>ОПК-15.8 владеет навыками работы с сетевым оборудованием и сетевым программным обеспечением.</p>   |
| ОПК-16  | <p>ОПК-16.6 Умеет формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе.</p> <p>ОПК-16.8 Умеет осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты.</p> <p>ОПК-16.10 Владеет методиками анализа сетевого трафика.</p> <p>ОПК-16.11 Знает основные виды деструктивных воздействий на программные продукты.</p> <p>ОПК-16.13 Знает современные методы анализа программных решений по обеспечению защищенности компьютерных систем.</p>  |
| ОПК-2.1 | <p>ОПК-2.1.1 Способен применять эффективные принципы разработки средств защиты информации с использованием актуальных математических методов.</p> <p>ОПК-2.1.2 Знает требования основных стандартов по защите компьютерных систем и сетей.</p> <p>ОПК-2.1.3 Способен разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при функционировании программно-аппаратных средств защиты информации.</p> <p>ОПК-2.1.4 Способен классифицировать информационные системы по требованиям защиты информации.</p> <p>ОПК-2.1.5 Способен разрабатывать программные алгоритмы с применением математических моделей для оценки безопасности компьютерных систем.</p>                                       |
| ОПК-2.2 | <p>ОПК-2.2.1 Применяет основные инструменты моделирования защищенных автоматизированных систем с целью анализа их уязвимостей.</p> <p>ОПК-2.2.2 Знает критерии эффективности систем защиты информации в объектах информатизации на базе компьютерных систем.</p> <p>ОПК-2.2.3 Знает основные алгоритмы кодирования сжатия и восстановления информации.</p> <p>ОПК-2.2.4 Проводит анализ средств и алгоритмов программного сжатия данных на предмет соответствия требованиям защиты информации.</p> <p>ОПК-2.2.5 Применяет средства и методы анализа компонентов системы безопасности с использованием современных математических методов.</p> <p>ОПК-2.2.6 Разрабатывает математические модели для оценки безопасности компьютерных систем.</p> |
| ОПК-2.3 | <p>ОПК-2.3.1 Знает современные и перспективные математические методы защиты информации.</p> <p>ОПК-2.3.2 Применяет основные методы инструментального анализа средств защиты информации.</p> <p>ОПК-2.3.3 Проводит оценку эффективности программных, программно-аппаратных и технических средств, подсистем защиты информации.</p> <p>ОПК-2.3.4 Формирует обоснование необходимости защиты информации в автоматизированной системе.</p>  |
| ПК-1    | <p>ПК-1.1 Применяет различные методы разработки программного обеспечения и технологии программирования.</p> <p>ПК-1.2 Использует современные математические методы и алгоритмы функционирования для компонентов программных средств.</p> <p>ПК-1.3 Применяет технологии обработки данных, анализирует возможности их использования при разработке программного обеспечения в профессиональной деятельности.</p>   |
| ПК-2    | <p>ПК-2.1 Применяет эффективные методы и средства планирования и организации исследований и разработок.</p> <p>ПК-2.2 Использует методы проведения экспериментов и наблюдений, обобщения и обработки информации, полученной в ходе исследований.</p> <p>ПК-2.3 Использует типовое и специализированное программное обеспечение, проводит компьютерное исследование, формирует описание результатов и формулирует выводы.</p> <p>ПК-2.4 Разрабатывает модели угроз безопасности информации и нарушителей.</p> <p>ПК-2.5 Проводит теоретические и экспериментальные исследования уровней защищенности информации в компьютерных системах и сетях.</p>   |

|      |  |
|------|--|
| ПК-3 | ПК-3.1 Формирует и применяет аналитическую модель эффективности внедрения средств защиты информации различных классов.<br>ПК-3.2 Осуществляет настройку ОС и настройку системы безопасности ОС в том числе и UNIX-систем.<br>ПК-3.3 Анализирует эффективность функционирования программных средств защиты информации.<br>ПК-3.4 Разрабатывает программные алгоритмы, реализующие современные математические методы защиты информации.<br>ПК-3.5 Выполняет анализ защищенности программных и программно-аппаратных средств защиты информации. |
|------|--|

## **12.5. 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.

## **12.6. Фонд оценочных средств для защиты ВКР**

### **12.6.1. 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 защищённости, 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?

### **12.6.2. 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 материал, презентация) | 2     | Раздаточный материал и/или презентация дают полное представление о 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   |

## Процедура 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.

## 12.7. 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: <a href="http://biblioclub.ru/index.php?page=book&amp;id=112247">http://biblioclub.ru/index.php?page=book&amp;id=112247</a> .  |
| 2.    | Новиков А.М., Новиков Д.А. Методология научного исследования. – М.: Либроком. 2010 – 280 с. URL: <a href="http://www.methodolog.ru/books/mni.pdf">http://www.methodolog.ru/books/mni.pdf</a> .  |
| 3.    | Мельников В. П., Клейменов С. А., Петраков А. М. Информационная безопасность и защита информации. - М.: Академия, 2007. – 330 с.  |
| 4.    | Основы управления информационной безопасностью: [учебное пособие для студентов вузов, обучающихся по направлениям подготовки (специальностям) укрупненной группы специальностей 090000 - "Информ. безопасность"] / А.П. Курило [и др.]. — 2-е изд., испр. — Москва: Горячая линия-Телеком, 2014. — 243 с. : ил., табл. — (Вопросы управления информационной безопасностью ; Кн.1) .— Библиогр.: с.234-239 .— ISBN 978-5-9912-0361-6.  |
| 5.    | Краковский, Ю.М. Информационная безопасность и защита информации: учебное пособие для студ. обуч. по специальности «Информационные системы и технологии» днев. и заоч. форм обучения / Ю.М. Краковский. — М.; Ростов н/Д : МарТ, 2008 .— 287 с. : ил .— (Учебный курс) .— Библиогр.: с.221 .— ISBN 978-5-241-00925-8.   |
| 6.    | Олейник П. П. Корпоративные информационные системы: для бакалавров и специалистов: учебник для студ. вузов, обуч. по направл. 080800 "Прикладная информатика (по областям)" и др. экон. спец. – СПб.: Питер, 2012. – 176 с.   |
| 7.    | Фостер, Джеймс. Защита от взлома: сокет, 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: <a href="http://e.lanbook.com/books/element.php?pl1_cid=25&amp;pl1_id=1117">http://e.lanbook.com/books/element.php?pl1_cid=25&amp;pl1_id=1117</a> >.   |
| 8.    | 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: <a href="http://e.lanbook.com/books/element.php?pl1_cid=25&amp;pl1_id=1112">http://e.lanbook.com/books/element.php?pl1_cid=25&amp;pl1_id=1112</a> >.   |
| 9.    | 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: <a href="http://www.lib.vsu.ru/elib/texts/method/vsu/may07045.pdf">http://www.lib.vsu.ru/elib/texts/method/vsu/may07045.pdf</a> >.  |
| 10.   | 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: <a href="http://e.lanbook.com/books/element.php?pl1_cid=25&amp;pl1_id=1118">http://e.lanbook.com/books/element.php?pl1_cid=25&amp;pl1_id=1118</a> >. |

|     |   |
|-----|---|
| 11. | Зайцев О.В. Rootkits, SpyWare/AdWare, Keyloggers & BackDoors: Обнаружение и защита / О.В. Зайцев. – СПб.: БХВ-Петербург, 2006. - 304 с.   |
| 12. | Проскурин В. Г. Защита программ и данных - М.: Академия, 2011. – 198 с.   |
| 13. | 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: <a href="http://www.intuit.ru/studies/courses/2196/267/info/">http://www.intuit.ru/studies/courses/2196/267/info/</a> . |
| 14. | Юрин И.Ю. Теоретические и практические основы защиты информации. 2012. <a href="http://library.sgu.ru/uch_lit/620.pdf">http://library.sgu.ru/uch_lit/620.pdf</a> .  |

б) дополнительная литература:

| № п/п | Источник  |
|-------|---|
| 15.   | Муромцева А. В. Искусство презентации. Основные правила и практические рекомендации / А.В. Муромцева. — Москва: Флинта: Наука, 2014. — 108 с.   |
| 16.   | Кручинин, В.В. Компьютерные технологии в научных исследованиях: учебно-методическое пособие / В.В. Кручинин. — Москва: ТУСУР (Томский государственный университет систем управления и радиоэлектроники), 2012. — 57 с. — Режим доступа: <a href="http://e.lanbook.com/books/element.php?pl1_id=11269">http://e.lanbook.com/books/element.php?pl1_id=11269</a> . |
| 17.   | 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: <a href="http://e.lanbook.com/books/element.php?pl1_id=28348">http://e.lanbook.com/books/element.php?pl1_id=28348</a> .  |
| 18.   | Системы и средства информатики: Ежегодник / Гл. ред. И.А. Соколов. — Москва: ИПИ РАН. — 2010.— Вып. 20. — № 2. — 350 с.   |
| 19.   | 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.   |
| 20.   | 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.   |
| 21.   | 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).  |
| 22.   | 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.  |
| 23.   | 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.                            |
| 24.   | Методический документ. Меры защиты информации в государственных информационных системах (утв. ФСТЭК России 11.02.2014).   |
| 25.   | 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.  |
| 26.   | Мещеряков В.А., Железняк В.П., Бондарь А.О., Осипенко А.Л., Бабкин А.Н. Персональные данные: организация обработки и обеспечения безопасности в органах государственной власти и местного самоуправления / Под ред. В.А. Мещерякова. – Воронеж: Воронежский институт МВД России, 2014. – 186 с.   |
| 27.   | 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.  |
| 28.   | Ермошкин Н.Н., Тарасов А.А. Стратегия информационных технологий предприятия. М.: Изд-во Московского гуманитарного университета, 2003.   |
| 29.   | Корнеев И.К., Степанов Е.А. Защита информации в офисе. – "Издательство Проспект", 2008. – 333 с.  |

|     |   |
|-----|---|
| 30. | Александр Доронин. Бизнес-разведка <a href="http://fxt.com.ua/business_literatura/131-aleksandr-doronin-biznes-razvedka.html">http://fxt.com.ua/business_literatura/131-aleksandr-doronin-biznes-razvedka.html</a> .  |
| 31. | Таненбаум Э. Компьютерные сети / Э. Таненбаум. – СПб.: Питер, 2005. — 991 с.  |
| 32. | Вялых А.С. Оценка возможностей атаки на информационную систему / А.С. Вялых, С.А. Вялых // Кибернетика и высокие технологии XXI века: матер. XII международ. науч.-тех. конф., Воронеж, 11-12 мая 2011 г. – Воронеж : ИПЦ ВГУ, 2011. – Т.1. – С. 91-96.   |
| 33. | Партыка Т.Л. Информационная безопасность М.: ФОРУМ, 2007.   |
| 34. | Мельников, Владимир Павлович. Информационная безопасность и защита информации: учебное пособие для студ. вузов, обуч. по специальности 230201 "Информационные системы и технологии" / В.П. Мельников, С.А. Клейменов, А.М. Петраков; под ред. С.А. Клейменова. — М. : АCADEMIA, 2006 .— 330 с. : ил. — (Высшее профессиональное образование. Информатика и вычислительная техника). — Библиогр.: с.327-328 .— ISBN 5-7695-2592-4. |
| 35. | Андрианов В.И. "Шпионские штучки" и устройства для защиты объектов, и информации: Справ. пособие / В.А.Бородин, А.В.Соколов. – С-Пб.: Лань, 1996.   |
| 36. | Абалмазов Э.И. Методы и инженерно – технические средства противодействия информационным угрозам / Э.И.Абалмазов. – М.: Гротек, 1997.  |
| 37. | Василевский И.В. Способы и средства предотвращения утечки информации по техническим каналам / И.В.Василевский. – М.: НПЦ "Нелк", 1998.  |
| 38. | Хорев А.А., Способы и средства ЗИ / А.А.Хорев. – МО РФ, 1998.   |
| 39. | 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.  |
| 40. | ИСО/МЭК 31000:2009 «Управление рисками. Принципы и направления», ISO Technical Management Board Working Group, 2009.  |
| 41. | ИСО/МЭК 31100:2009 «Управление рисками. Методики оценки риска», ISO Technical Management Board Working Group, 2009.   |
| 42. | 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  |
|-------|---|
| 43.   | ЭБС Лань  |
| 44.   | ЭБС «Университетская библиотека online»   |
| 45.   | ЭБС «Электронная библиотека технического ВУЗа» (ЭБС «Консультант студента»)   |
| 46.   | ЭБС ЮРАЙТ   |
| 47.   | Электронная библиотека учебно-методических материалов ВГУ. Режим доступа: <a href="http://www.lib.vsu.ru">http://www.lib.vsu.ru</a> |
| 48.   | <a href="http://www.cryptopro.ru">http://www.cryptopro.ru</a>   |
| 49.   | <a href="http://www.infotecs.ru">http://www.infotecs.ru</a>   |
| 50.   | <a href="http://www.lissi-crypto.ru/">http://www.lissi-crypto.ru/</a>   |
| 51.   | <a href="http://www.signal-com.ru">http://www.signal-com.ru</a>   |
| 52.   | <a href="http://www.shipka.ru">http://www.shipka.ru</a>   |

Обучающийся дополнительно использует литературу, соответствующую тематике ВКР.

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

Образовательный портал «Электронный университет ВГУ».

Электронные библиотечные системы:

– ЭБС «Университетская библиотека online».

– ЭБС «Лань».



Программное обеспечение:

ОС Windows 10, ОС Linux, пакет стандартных офисных приложений для работы с документами, таблицами и т.п. (MS Office, МойОфис, LibreOffice), ПО Adobe Reader, интернет-браузер (Google Chrome, Mozilla Firefox); ПО Free Pascal, Microsoft Visual Studio Community Edition, ПО Anylogic, Python (допускается замена специализированного ПО виртуальным аналогом).

Подключение к сети Internet для демонстрации практической составляющей ВКР ориентированных на построение сайтов или использование технологий Internet.

### **12.9. Материально-техническое обеспечение:**

Специализированная мебель, компьютер (ноутбук), мультимедийное оборудование (проектор, экран, средства звуковоспроизведения).

### **13. Особенности проведения ГИА для лиц с ограниченными возможностями здоровья и инвалидов**

Для обучающихся из числа лиц с ограниченными возможностями здоровья и инвалидов ГИА проводится с учётом особенностей их психофизического развития, их индивидуальных возможностей и состояния здоровья, а также в соответствии с требованиями, изложенными в пункте 7 Положения 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.