

Министерство науки и высшего образования Российской Федерации  
федеральное государственное автономное образовательное учреждение  
высшего образования «Самарский национальный исследовательский  
университет имени академика С.П. Королева»



**САМАРСКИЙ** УНИВЕРСИТЕТ  
SAMARA UNIVERSITY

УТВЕРЖДЕН

25 июня 2021 года, протокол ученого совета  
университета №12  
Сертификат №: 1a 73 60 dc 00 01 00 00 03 34  
Срок действия: с 26.02.2021г. по 26.02.2022г.  
Владелец: проректор по учебной работе  
А. В. Гаврилов

**ПРОГРАММА**  
**ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ**

Код плана	<u>100503-2021-О-ПП-5г06м-01</u>
Основная профессиональная образовательная программа высшего образования по направлению подготовки (специальности)	<u>10.05.03 Информационная безопасность автоматизированных систем</u>
Профиль (программа, специализация)	<u>Специализация № 5 "Безопасность открытых информационных систем"</u>
Квалификация (степень)	<u>Специалист по защите информации</u>
Блок, в рамках которого проводится государственная итоговая аттестация	<u>БЗ</u>
Институт (факультет)	<u>Институт информатики и кибернетики</u>
Кафедра	<u>геоинформатики и информационной безопасности</u>
Форма обучения	<u>очная</u>
Курс, семестр	<u>6 курс, 11 семестр</u>
Форма (формы) государственной итоговой аттестации	<u>защита выпускной квалификационной работы</u>

Самара, 2021



Настоящая программа государственной итоговой аттестации является составной частью основной профессиональной образовательной программы высшего образования Безопасность открытых информационных систем по специальности 10.05.03 Информационная безопасность автоматизированных систем, обеспечивающей реализацию федерального государственного образовательного стандарта высшего образования - специалитет по специальности 10.05.03 Информационная безопасность автоматизированных систем, утвержденного приказом Минобрнауки России от 26.11.2020 N 1457.

Составители:

Заведующий кафедрой геоинформатики  
и информационной безопасности



*В.В. Сергеев*

«\_\_» \_\_\_\_\_ 20\_\_ г.

Программа государственной итоговой аттестации обсуждена на заседании кафедры геоинформатики и информационной безопасности

Протокол №4 от «17» марта\_\_ 2021 г.

Руководитель основной образовательной  
программы высшего образования:  
Безопасность открытых информационных  
систем 10.05.03 Информационная  
безопасность автоматизированных систем



*В.В. Сергеев*

Настоящая программа государственной итоговой аттестации является составной частью основной профессиональной образовательной программы высшего образования Безопасность открытых информационных систем по специальности 10.05.03 Информационная безопасность автоматизированных систем, обеспечивающей реализацию федерального государственного образовательного стандарта высшего образования - специалитет по специальности 10.05.03 Информационная безопасность автоматизированных систем, утвержденного приказом Минобрнауки России от 26.11.2020 N 1457.

Составители:

Заведующий кафедрой геоинформатики  
и информационной безопасности

*В.В. Сергеев*

«\_\_» \_\_\_\_\_ 20\_\_ г.

Программа государственной итоговой аттестации обсуждена на заседании кафедры геоинформатики и информационной безопасности

Протокол №4 от «17» марта 2021 г.

Руководитель основной образовательной  
программы высшего образования:  
Безопасность открытых информационных  
систем 10.05.03 Информационная  
безопасность автоматизированных систем

*В.В. Сергеев*

## 1. ОБЩАЯ ХАРАКТЕРИСТИКА ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

Государственная итоговая аттестация (далее – ГИА) представляет собой форму оценки степени и уровня освоения обучающимися образовательной программы. ГИА проводится на основе принципов объективности и независимости оценки качества подготовки обучающихся.

ГИА проводится государственными экзаменационными комиссиями (далее – ГЭК). Для рассмотрения апелляций по результатам ГИА в Самарском университете (далее – университет) создаются апелляционные комиссии. Регламент работы государственной экзаменационной комиссии и апелляционной комиссии (далее вместе – комиссии) установлены локальными нормативными актами университета.

ГИА проводится в целях определения соответствия результатов освоения обучающимися основной профессиональной образовательной программы высшего образования Безопасность открытых информационных систем ПО специальности 10.05.03 Информационная безопасность автоматизированных систем, соответствующим требованиям федерального государственного образовательного стандарта высшего образования - специалитет по специальности 10.05.03 Информационная безопасность автоматизированных систем, утвержденного приказом Минобрнауки России от 26.11.2020 N 1457.

ГИА, завершающая освоение настоящей основной профессиональной образовательной программы высшего образования (далее – ОПОП ВО), является обязательной и проводится в порядке и в форме, которые установлены законодательством об образовании, настоящей программой и иными локальными нормативными актами университета, регулирующими вопросы организации и проведения ГИА.

Содержание и характеристика формы (вида) государственных аттестационных испытаний приведены в таблице 1.

*Таблица 1. Содержание и характеристика формы (вида) государственных аттестационных испытаний*

Форма проведения ГИА	Содержание ГИА	Характеристика формы (вида) государственного аттестационного испытания
Защита выпускной квалификационной работы	Подготовка к процедуре защиты и защита выпускной квалификационной работы	выпускная квалификационная работа

Настоящая программа ГИА, включая требования к выпускным квалификационным работам (далее – ВКР) и порядку их выполнения, критерии оценки результатов защиты ВКР, утвержденные университетом, а также порядок подачи и рассмотрения апелляций доводятся до сведения обучающихся не позднее чем за шесть месяцев до начала ГИА.

## 2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОСВОЕНИЯ ОПОП ВО В СООТВЕТСТВИИ С ТРЕБОВАНИЯМИ ФГОС ВО И ОПОП ВО

Планируемые результаты освоения ОПОП ВО – это компетенции, установленные ФГОС ВО, и дополнительные профессиональные компетенции, установленные университетом в ОПОП ВО.

Планируемые результаты освоения ОПОП ВО – это компетенции, установленные в ОПОП ВО, которые определены

- в соответствии с ФГОС ВО,
- в соответствии с профессиональными стандартами, соответствующими профессиональной деятельности выпускников
- на основе анализа требований к профессиональным компетенциям, предъявляемых к выпускникам на рынке труда, обобщения отечественного и зарубежного опыта, проведения консультаций с ведущими работодателями, объединениями работодателей отрасли, в которой востребованы выпускники, иных источников.

Перечень планируемых результатов освоения ОПОП ВО приведен в таблице 2.

Таблица 2. Перечень планируемых результатов освоения ОПОП ВО

Код компетенции	Содержание компетенции
<i>Универсальные компетенции (УК)</i>	
УК-1	Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий
УК-2	Способен управлять проектом на всех этапах его жизненного цикла
УК-3	Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели
УК-4	Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия
УК-5	Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия
УК-6	Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни
УК-7	Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности
УК-8	Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов
УК-9	Способен принимать обоснованные экономические решения в различных областях жизнедеятельности
УК-10	Способен формировать нетерпимое отношение к коррупционному поведению
<i>Общепрофессиональные компетенции (ОПК)</i>	
ОПК-1	Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;

Код компетенции	Содержание компетенции
ОПК-2	Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности;
ОПК-3	Способен использовать математические методы, необходимые для решения задач профессиональной деятельности;
ОПК-4	Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности;
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 автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;
ОПК-7	Способен создавать программы на языках общего назначения, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ;
ОПК-8	Способен применять методы научных исследований при проведении разработок в области защиты информации в автоматизированных системах;
ОПК-9	Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации;
ОПК-10	Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности;
ОПК-11	Способен разрабатывать компоненты систем защиты информации автоматизированных систем;
ОПК-12	Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем;
ОПК-13	Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем;
ОПК-14	Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений;
ОПК-15	Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем;

Код компетенции	Содержание компетенции
ОПК-16	Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма.
<i>Общепрофессиональные компетенции специализации</i>	
ОПК-5.1	Способен разрабатывать и реализовывать политику информационной безопасности открытых информационных систем;
ОПК-5.2	Способен разрабатывать и эксплуатировать системы защиты информации открытых информационных систем;
ОПК-5.3	Способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах;
<i>Профессиональные компетенции (ПК)</i>	
ПК-1	Способен выполнять интеграцию программных модулей и компонент, проводить верификацию программных продуктов
ПК-2	Способен разрабатывать требования и проектировать программное обеспечение
ПК-3	Способен разрабатывать системные утилиты и компоненты операционной системы
ПК-4	Способен разрабатывать системы защиты информации автоматизированных систем
ПК-5	Способен осуществлять непосредственное руководство процессами разработки программного обеспечения
ПК-6	Способен оценивать уровень безопасности компьютерных систем и сетей
ПК-7	Способен применять методы анализа данных для решения задач информационной безопасности
ПК-8	Способен разрабатывать и использовать методы защиты данных, хранящихся и передаваемых в автоматизированных системах

### 3. УКАЗАНИЕ ОБЪЕМА ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ В ЗАЧЕТНЫХ ЕДИНИЦАХ И ЕЕ ПРОДОЛЖИТЕЛЬНОСТИ В НЕДЕЛЯХ И В АКАДЕМИЧЕСКИХ ЧАСАХ

Объем ГИА и продолжительность ее проведения приведены в таблице 3.

*Таблица 3. Объем государственной итоговой аттестации в зачетных единицах и ее продолжительность*

Наименования показателей, характеризующих объем и продолжительность ГИА	Значение показателей объема и продолжительности ГИА
Семестр	11
Количество зачетных единиц	6
Количество недель	4
Количество академических часов на подготовку к процедуре защиты и защиту выпускной квалификационной работы	216
контролируемая самостоятельная работа (контроль готовности ВКР просмотровой комиссией кафедры), академических часов	2
самостоятельная работа (подготовка к защите ВКР), академических часов	178
контроль (защита ВКР, включая подготовку к процедуре защиты), академических часов	36

### 4. СТРУКТУРА И СОДЕРЖАНИЕ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

ГИА включает ряд этапов, необходимых для организации и проведения государственных аттестационных испытаний, предусмотренных ОПОП ВО в соответствии с ФГОС ВО. Структура и содержание этапов ГИА приведены в таблице 4.

Таблица 4. Структура и содержание этапов ГИА

Этапы подготовки и проведения ГИА	Содержание этапа
1. Подготовительный (организационный) этап к процедуре ГИА	<p>Утверждение председателя ГЭК.            Утверждение состава ГЭК.            Утверждение программы ГИА по ОПОП ВО.            Утверждение перечня тем ВКР по ОПОП ВО.            Доведение до сведения обучающихся программы ГИА и утвержденного перечня тем ВКР по ОПОП ВО не позднее чем за шесть месяцев до начала ГИА.            Закрепление за обучающимися тем ВКР (на основании их личных заявлений), руководителей ВКР и, при необходимости, консультанта (консультантов) приказом ректора или уполномоченного им лица до начала преддипломной практики.            Утверждение распорядительным актом расписания государственных аттестационных испытаний не позднее, чем за 30 календарных дней до дня проведения первого государственного аттестационного испытания.            Доведение расписания государственных аттестационных испытаний до сведения обучающихся, председателя, членов и секретаря ГЭК, руководителей и консультантов ВКР.            Организация работы комиссии.</p>
2. Подготовка к защите ВКР	<p>Представление руководителю для проверки полного текста ВКР.            Устранение замечаний (при необходимости).            Подготовка доклада о результатах ВКР и раздаточного материала, иллюстрирующего содержание доклада о результатах ВКР.            Предоставление доклада и раздаточного материала руководителю ВКР. Устранение замечаний (при необходимости).            Оформление текста ВКР. Нормоконтроль оформления текста ВКР.            Проверка текста ВКР на объем заимствования.            Ознакомление обучающегося с отзывом руководителя на ВКР, рецензией не позднее чем за 5 календарных дней до дня защиты ВКР.            Предварительный просмотр ВКР на кафедре. Получение заключения просмотрной комиссии выпускающей кафедры по результатам просмотра ВКР. Устранение замечаний (при необходимости).            Размещение текстов ВКР в электронно-библиотечной системе университета через личный кабинет обучающегося.            Передача в ГЭК ВКР, отзыва и рецензии не позднее чем за 2 календарных дня до дня защиты ВКР.</p>
3. Процедура защиты ВКР	<p>Процедура защиты ВКР включает в себя:</p> <ul style="list-style-type: none"> <li>– открытие заседания ГЭК председателем ГЭК;</li> <li>– доклад обучающегося;</li> <li>– вопросы членов ГЭК;</li> <li>– заслушивание отзыва руководителя ВКР;</li> <li>– заслушивание рецензии на ВКР</li> <li>– заключительное слово обучающегося.</li> </ul>
4. Заключительный (организационный) этап процедуры ГИА	<p>Оформление протоколов заседаний ГЭК по результатам каждого заседания ГЭК в соответствии с утвержденным расписанием государственных аттестационных испытаний.            Оформление книг протоколов заседаний ГЭК.            Сдача протоколов заседаний ГЭК на хранение в архив университета.</p>

## 5. ТРЕБОВАНИЯ К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ И ПОРЯДКУ ЕЕ ВЫПОЛНЕНИЯ

### 5.1. Требования к структуре, объему и содержанию выпускной квалификационной работы

Структурными элементами текста ВКР в соответствии со стандартом Самарского университета «Общие требования к учебным текстовым документам» являются:

- титульный лист ВКР (оформляется на бланке университета и служит обложкой ВКР);
- задание (оформляется на типовом бланке);
- содержание (включает введение, наименование всех разделов и подразделов (если имеются), заключение, список использованных источников, приложения (при наличии) с указанием номеров страниц, с которых начинаются эти структурные элементы ВКР);
- введение (актуальность, цель, задачи, предмет и объект исследования, содержание проблемы, личный вклад автора в её решение, методология и избранные методы исследования, научная новизна, практическая значимость, область применения результатов);
- основная часть (определяется кафедрой, выдавшей задание, в соответствии с ФГОС ВО);
- заключение (выводы и результаты работы, полученный научно-технический и социально-экономический эффект, задачи, оставшиеся нерешёнными, и пути их решения в дальнейшем при использовании результатов работы);
- список использованных источников (включает все использованные источники: книги, статьи из журналов и сборников, авторские свидетельства, государственные стандарты и прочие сведения, которые оформляются в соответствии с требованиями ГОСТ);
- приложения (оформляются при наличии материалов, которые не являются самой работой, но способствуют её обоснованности).

Структура ВКР может уточняться обучающимся совместно с научным руководителем в целях раскрытия темы.

Рекомендуемый объем ВКР обучающегося – 40 страниц печатного текста, исключая листы задания, реферата, содержания, рисунки, таблицы, схемы, список использованных источников и приложения.

Основная часть ВКР, как правило, состоит из трех разделов:

Глава 1. Постановка задачи и обоснование метода решения задачи

1.1. Описание предметной области и постановка задачи.

1.2. Анализ существующих методов решения задачи и обоснование выбора реализуемого метода.

1.3. Обзор имеющихся аналогов систем, технологий, вариантов решения задачи.

Глава 2. Решение поставленной задачи.

2.1. Обоснование и выбор комплекса программных или технических средств, языка программирования, операционной системы и специализированного программного обеспечения, состава приборов или оборудования (при необходимости).

2.2. Описание структуры, информационно-логической модели автоматизированной системы, модели угроз и т.п. (при необходимости),

2.3. Разработка алгоритмов обработки данных или методики проводимых измерений.

Глава 3. Экспериментальная часть.

3.1. Составление методики и плана исследований эффективности программно-технической разработки по теме ВКР.

3.2. Проведение, обработка и анализ результатов экспериментальных измерений (при необходимости).

3.3. Проведение вычислительных экспериментов для исследования эффективности разработанных методов, программных средств и/или автоматизированной системы на модельных или реальных данных (при необходимости).

Качество и сроки выполнения этапов ВКР контролирует руководитель ВКР из числа работников университета. После завершения подготовки обучающимся ВКР руководитель ВКР представляет в университет на кафедру письменный отзыв о работе обучающегося в период подготовки ВКР.

## 5.2. Требования к оформлению выпускной квалификационной работы

Оформление ВКР осуществляется в соответствии со стандартом Самарского университета «Общие требования к учебным текстовым документам».

## 6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ВКЛЮЧАЯ ПЕРЕЧЕНЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, НЕОБХОДИМОГО ДЛЯ ПРОВЕДЕНИЯ ГИА

### 6.1. Описание материально-технической базы

Материально-техническая база, необходимая для подготовки к ГИА и проведения ГИА, обеспечена специальными помещениями – учебными аудиториями для проведения групповых и индивидуальных консультаций, проведения ГИА, а также помещениями для самостоятельной работы и помещениями для хранения и профилактического обслуживания учебного оборудования.

Контактная работа с руководителем ВКР и консультантом (консультантами) (при наличии) проходит в аудитории, оснащенной презентационной техникой (проектор, экран, компьютер/ноутбук), учебной мебелью: столы, стулья для обучающихся; стол, стул для преподавателя.

Для самостоятельной работы обучающегося предоставляется компьютерный класс, оснащенный компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду университета.

При проведении ГИА используется презентационная техника (проектор, экран, компьютер/ноутбук), учебно-наглядные пособия (презентационные материалы).

Организовано асинхронное взаимодействие обучающегося и руководителя ВКР (консультантов при их наличии) с использованием электронной информационной образовательной среды университета через систему личных кабинетов обучающихся и преподавателей. Обучающийся размещает в личном кабинете ВКР, РУКОВОДИТЕЛЬ ВКР-отзыв руководителя ВКР, рецензию на ВКР. Руководитель ВКР проверяет и верифицирует размещенные ВКР, отзыв руководителя ВКР, рецензию на ВКР. После этого ВКР, отзыв и рецензия сохраняются в электронном портфолио обучающегося и в электронной библиотечной системе университета.

Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к одной или нескольким электронно-библиотечным системам (электронным библиотекам) и к электронной информационно-образовательной среде организации (<http://lib.ssau.ru/els>). Электронно-библиотечная система (электронная библиотека) и электронная информационно-образовательная среда обеспечивает возможность доступа обучающегося из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети «Интернет», как на территории университета, так и вне ее.

### 6.2 Перечень лицензионного программного обеспечения

Таблица 5. Лицензионное программное обеспечение, необходимые для подготовки к ГИА

№ п/п	Наименование	Тип и реквизиты ресурса
1.	MS Windows 8 (Microsoft)	ГК № ЭА-26/13 от 25.06.2013
2.	MS Windows 10 (Microsoft)	Microsoft Open License №68795503 от 18.08.2017, Microsoft Open License №68795512 от 18.08.2017,

		Договор № ЭА-113/16 от 28.11.2016, Договор № ЭА-24/17 от 24.08.2017
3.	MS Office 2013 (Microsoft)	Microsoft Open License №61308915 от 19.12.2012 ГК № ЭА-26/13 от 25.06.2013
4.	Visual Studio (Microsoft)	ГК № ЭА-26/13 от 25.06.2013
5.	MATLAB (Mathworks) Image Processing Toolbox (Mathworks) Statistics Toolbox (Mathworks)	-ГК № ЭА-26/13 от 25.06.2013; -ГК № ЭА-75/14 от 01.12.2014; -ГК № ЭА-89/14 от 23.12.2014;
6.	КриптоАРМ ("Цифровые Технологии")	ГК № ЭА – 38/14 от 22.07.2014.
7.	Horizon View (Vmware)	ГК № ЭА – 38/14 от 22.07.2014, ГК № ЭА-75/14 от 01.12.2014, Договор № ЭА-113/16 от 28.11.2016, Договор № ЭА-24/17 от 24.08.2017

### 6.3 Перечень свободно распространяемого программного обеспечения

1. FireFox
2. Google Chrome
3. ОС CentOS
4. ОС Ubuntu
5. Microsoft SQL Server Express Edition
6. MySQL Community Server
7. PostgreSQL
8. СПС КонсультантПлюс
9. Python
10. Apache Spark
11. Docker
12. IDA Freeware
13. Java SE Development Kit
14. Клеопатра
15. Microsoft Visual Studio Community Edition
16. Packet Tracer
17. PyCharm IDE Community Edition
18. Spyder IDE
19. TeX Live
20. TeXStudio
21. Zotero
22. .NET
23. Apache OpenOffice
24. LibreOffice

в том числе перечень свободно распространяемого программного обеспечения отечественного производства:

1. Яндекс. Браузер.

## 7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ГИА

### 7.1. Основная литература

1. Родичев, Ю. А. Нормативная база и стандарты в области информационной безопасности [Текст] : [учеб. пособие по направлению подгот. 10.00.00 "Информ. безопасность"]. – Питер, 2017. – 254 с.
2. Информатика [Текст] : базовый курс : [учеб. пособие для вузов]. – СПб. ; М. ; Нижний Новгород.: Питер, 2015. – 637 с.
3. Щеглов, А. Ю. Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. – М. : Издательство Юрайт, 2019. – 309 с. – (Серия : Бакалавр и магистр. Академический курс). – ISBN 978-5-534-04732-5. – Режим доступа: <https://www.biblio-online.ru/book/zaschita-informacii-osnovy-teorii-433715>
4. Шкляр, М.Ф. Основы научных исследований : учебное пособие / М.Ф. Шкляр. – 6-е изд. – Москва : Издательско-торговая корпорация «Дашков и К°», 2017. – 208 с. ; То же [Электронный ресурс]. – Режим доступа: <http://biblioclub.ru/index.php?page=book&id=450782>

#### 7.2. Дополнительная литература. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по подготовке к ГИА

1. Оформление результатов научной работы [Электронный ресурс]. – 2011. – on-line
2. Галатенко, В. А. Стандарты информационной безопасности: курс лекций : учеб. пособие : [для вузов по специальностям в обл. информ. технологий]. – М.: ИНТУИТ.ру, 2006. – 263 с.
3. Основы информационной безопасности : [учеб. пособие для вузов]. – Старый Оскол: ТНТ, 2017. – 381 с.
4. Бабаш, А. В. Криптографические методы защиты информации. – Т. 1 . – 2016. Т. 1 . – 413 с.
5. Олифер, В. Г. Сетевые операционные системы: [учеб. пособие для вузов по направлению подгот. дипломир. специалистов "Информатика и вычисл. техника]. – СПб., М., Нижний Новгород.: Питер, Питер Пресс, 2007. – 538 с.
6. Правовое обеспечение информационной безопасности: учебник для вузов. – М.: Маросейка, 2008. – 368 с.
7. Моисеев, А. И. Информационная безопасность распределенных информационных систем [Электронный ресурс] : учеб. по специальности "Информ. безопасность автоматизир. сис. – Самара.: [Изд-во СГАУ], 13. – on-line
8. Миркин Б.Г. Введение в анализ данных: учебник и практикум / Б. Г. Миркин. – Москва: Юрайт, 2017. —174 с.

7.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для подготовки к ГИА

Таблица 6. Ресурсы информационно-телекоммуникационной сети «Интернет», необходимые для подготовки к ГИА

№ п/п	Наименование ресурса	Адрес	Тип доступа
1	<a href="http://cyberleninka.ru">http://cyberleninka.ru</a>	Открытая электронная библиотека «Киберленинка»	Открытый ресурс
2	<a href="https://bdu.fstec.ru/threat">https://bdu.fstec.ru/threat</a>	Банк данных угроз безопасности информации ФСТЭК России	Открытый ресурс
3	<a href="https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty">https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty</a>	Актуальные версии нормативно-методических документов ФСТЭК России, применяемых при организации работ по защите информации в автоматизированных системах	Открытый ресурс
4	<a href="https://archive.neicon.ru/xmlui/">https://archive.neicon.ru/xmlui/</a>	Архив научных журналов на платформе НЭИКОН	Открытый ресурс

7.4. Перечень информационных справочных систем и современных профессиональных баз данных, необходимых для подготовки к ГИА

Таблица 7. Информационные справочные системы, необходимые для подготовки к ГИА

№ п/п	Наименование ресурса	Тип и реквизиты ресурса
1.	СПС КонсультантПлюс	Информационная справочная система, Договор №ЭЖ-89/18 от 20.12.2018
2.	Система интегрированного поиска EBSCO Discovery Service EBSCO Publishing	Информационная справочная система, №156-EBSCO/19 от 11.12.2018

Таблица 8. Современные профессиональные базы данных, необходимые для подготовки к ГИА

№ П/п	Наименование ресурса	Тип и реквизиты ресурса
1.	Электронная библиотека диссертаций (ЭБД РГБ)	Профессиональная база данных, №095040156 от 29.11.2018
2.	Электронно-библиотечная система eLibrary (журналы)	Профессиональная база данных, №1545 от 6.12.2018
3.	Полнотекстовая электронная библиотека	Профессиональная база данных, ГК №ЭА 14-12 от 10.05.2012
4.	Наукометрическая (библиометрическая) БД Web of Science	Профессиональная база данных, № WoS 968 от 02.04.2018
5.	Наукометрический пакет Incites	Профессиональная база данных, Договор № 156-18WOS
6	Аналитическая база данных «SciVal» издательства Elsevier	Профессиональная база данных, №1554 от 11.12.2018

## 8. КРИТЕРИИ ОЦЕНКИ РЕЗУЛЬТАТОВ ЗАЩИТЫ ВЫПУСКНЫХ КВАЛИФИКАЦИОННЫХ РАБОТ

Критерии оценки результатов защиты ВКР приведены в фонде оценочных средств для проведения ГИА (Приложение 2 к настоящей программе).

## 9. ПОРЯДОК ПРОВЕДЕНИЯ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ ДЛЯ ВЫПУСКНИКОВ ИЗ ЧИСЛА ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Для обучающихся из числа инвалидов ГИА проводится с учетом особенностей их психофизического развития, их индивидуальных возможностей и состояния здоровья (далее – индивидуальные особенности).

При проведении ГИА обеспечивается соблюдение следующих общих требований:

- проведение ГИА для инвалидов в одной аудитории совместно с обучающимися, не являющимися инвалидами, если это не создает трудностей для инвалидов и иных обучающихся при прохождении ГИА;

- присутствие в аудитории ассистента (ассистентов), оказывающего обучающимся инвалидам необходимую техническую помощь с учетом их индивидуальных особенностей (занять рабочее место, передвигаться, прочитать и оформить задание, общаться с председателем и членами ГЭК);

- пользование необходимыми обучающимся инвалидам техническими средствами при прохождении ГИА с учетом их индивидуальных особенностей;

- обеспечение возможности беспрепятственного доступа обучающихся инвалидов в аудитории, туалетные и другие помещения, а также их пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных проемов, лифтов, при отсутствии лифтов аудитория должна располагаться на первом этаже, наличие специальных кресел и других приспособлений).

Все локальные нормативные акты университета по вопросам проведения ГИА доводятся до сведения обучающихся инвалидов в доступной для них форме.

По письменному заявлению обучающегося инвалида продолжительность сдачи обучающимся инвалидом государственного аттестационного испытания может быть увеличена по отношению к установленной продолжительности его сдачи:

- продолжительность выступления обучающегося при защите ВКР – не более чем на 15 минут.

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

а) для слепых:

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

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

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

б) для слабовидящих:

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

- обеспечивается индивидуальное равномерное освещение не менее 300 люкс;

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

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

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

– по желанию обучающихся государственное аттестационное испытание проводится в письменной форме;

г) для лиц с нарушениями опорно-двигательного аппарата (тяжелыми нарушениями двигательных функций верхних конечностей или отсутствием верхних конечностей):

– письменные задания выполняются обучающимися на компьютере со специализированным программным обеспечением или надиктовываются ассистенту;

– по желанию обучающихся государственные аттестационные испытания проводятся в устной форме.

Обучающийся из числа инвалидов не позднее чем за 3 месяца до начала проведения ГИА подает письменное заявление о необходимости создания для него специальных условий при проведении государственных аттестационных испытаний с указанием его индивидуальных особенностей в Центр инклюзивного образования университета. К заявлению прилагаются документы, подтверждающие наличие у обучающегося индивидуальных особенностей (при отсутствии указанных документов в университете).

В заявлении обучающийся из числа инвалидов указывает на необходимость (отсутствие необходимости) присутствия ассистента на государственном аттестационном испытании, необходимость (отсутствие необходимости) увеличения продолжительности сдачи государственного аттестационного испытания по отношению к установленной продолжительности.

федеральное государственное автономное образовательное учреждение высшего образования «Самарский национальный исследовательский университет имени академика С.П. Королева»  
(Самарский университет)



**САМАРСКИЙ УНИВЕРСИТЕТ**  
SAMARA UNIVERSITY

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ  
ДЛЯ ПРОВЕДЕНИЯ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ**

Код плана	<u>100503-2021-О-ПП-5г06м-01</u>
Направление подготовки (специальность)	<u>10.05.03 Информационная безопасность автоматизированных систем</u>
Профиль (направленность) образовательной программы	<u>специализация N 5 " Безопасность открытых информационных систем "</u> ,
Квалификация	Специалист по защите информации
Блок, в рамках которого проводится государственная итоговая аттестация	<u>БЗ</u>
Институт (факультет)	<u>Институт информатики, математики и электроники</u>
Кафедра	<u>геоинформатики и информационной безопасности</u>
Форма обучения, год набора	<u>очная, набор 2021 года</u>
Курс, семестр	<u>5 курс, семестр 11</u>
Формы государственной итоговой аттестации	<u>Защита выпускной квалификационной работы</u>

Самара 2021

1. ПЕРЕЧЕНЬ КОМПЕТЕНЦИЙ, КОТОРЫМИ ДОЛЖНЫ ОВЛАДЕТЬ ОБУЧАЮЩИЕСЯ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Таблица 1. Компетенции, которыми должны овладеть обучающиеся в результате освоения образовательной программы, соотнесенные с формами ГИА

Код компетенции	Содержание компетенции	Формы ГИА
УК-1	Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	Защита ВКР
УК-2	Способен управлять проектом на всех этапах его жизненного цикла	Защита ВКР
УК-3	Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	Защита ВКР
УК-4	Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	Защита ВКР
УК-5	Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	Защита ВКР
УК-6	Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни	Защита ВКР
УК-7	Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности	Защита ВКР
УК-8	Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов	Защита ВКР
УК-9	Способен принимать обоснованные экономические решения в различных областях жизнедеятельности	Защита ВКР
УК-10	Способен формировать нетерпимое отношение к коррупционному поведению	Защита ВКР
ОПК-1	Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;	Защита ВКР
ОПК-2	Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для	Защита ВКР

Код компетенции	Содержание компетенции	Формы ГИА
	решения задач профессиональной деятельности;	
ОПК-3	Способен использовать математические методы, необходимые для решения задач профессиональной деятельности;	Защита ВКР
ОПК-4	Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности;	Защита ВКР
ОПК-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;	Защита ВКР
ОПК-6	Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	Защита ВКР
ОПК-7	Способен создавать программы на языках общего назначения, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ;	Защита ВКР
ОПК-8	Способен применять методы научных исследований при проведении разработок в области защиты информации в автоматизированных системах;	Защита ВКР
ОПК-9	Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации;	Защита ВКР
ОПК-10	Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности;	Защита ВКР
ОПК-11	Способен разрабатывать компоненты систем защиты информации автоматизированных систем;	Защита ВКР

Код компетенции	Содержание компетенции	Формы ГИА
ОПК-12	Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем;	Защита ВКР
ОПК-13	Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем;	Защита ВКР
ОПК-14	Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений;	Защита ВКР
ОПК-15	Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем;	Защита ВКР
ОПК-16	Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма.	Защита ВКР
ОПК-5.1	Способен разрабатывать и реализовывать политику информационной безопасности открытых информационных систем;	Защита ВКР
ОПК-5.2	Способен разрабатывать и эксплуатировать системы защиты информации открытых информационных систем;	Защита ВКР
ОПК-5.3	Способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах;	Защита ВКР
ПК-1	Способен выполнять интеграцию программных модулей и компонент, проводить верификацию программных продуктов	Защита ВКР
ПК-2	Способен разрабатывать требования и проектировать программное обеспечение	Защита ВКР
ПК-3	Способен разрабатывать системные утилиты и компоненты операционной системы	Защита ВКР
ПК-4	Способен разрабатывать системы защиты информации автоматизированных систем	Защита ВКР
ПК-5	Способен осуществлять непосредственное руководство процессами разработки программного обеспечения	Защита ВКР

Код компетенции	Содержание компетенции	Формы ГИА
ПК-6	Способен оценивать уровень безопасности компьютерных систем и сетей	Защита ВКР
ПК-7	Способен применять методы анализа данных для решения задач информационной безопасности	Защита ВКР
ПК-8	Способен разрабатывать и использовать методы защиты данных, хранящихся и передаваемых в автоматизированных системах	Защита ВКР

## 2. ОПИСАНИЕ ПОКАЗАТЕЛЕЙ И КРИТЕРИЕВ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ, А ТАКЖЕ ШКАЛ ОЦЕНИВАНИЯ

2.1 Показатели и критерии оценивания сформированности компетенций при проведении защиты выпускной квалификационной работы

Оценивание ВКР осуществляется в два этапа:

1. Предварительное оценивание ВКР – осуществляется руководителем ВКР обучающегося (отзыв руководителя ВКР, рецензией).
2. Оценка результатов защиты ВКР членами ГЭК) – итоговая оценка выставляется на основании результатов экспертной оценки членов ГЭК (Таблица 2).

Таблица 2. Показатели оценивания сформированности компетенций при проведении защиты ВКР

Показатели оценки защиты ВКР	Коды компетенций	Удельный вес показателя	Отлично	Хорошо	Удовлетворительно	Неудовлетворительно
			5	4	3	2
1. Обоснованность проблемы, постановка цели, выделение основных задач, объекта и предмета исследования	УК-1, ОПК-1, ОПК-3, ОПК-4, ОПК-9, ОПК-11, ОПК-13, ОПК-14, ОПК-15 ПК-1, ПК-4, ПК-7	0,1	5	4	3	2
2. Уровень теоретической, научно-исследовательской и практической проработки проблемы	УК-2, ОПК-2, ОПК-3, ОПК-4, ОПК-7, ОПК-8, ОПК-12 ПК-1, ПК-5, ПК-8	0,2	5	4	3	2
3. Качество анализа проблемы, наличие и качество вносимых предложений по совершенствованию качества проекта и программной реализации метода решения проблемы, оценка эффективности рекомендаций	УК-2, ОПК-1, ОПК-5, ОПК-6, ОПК-5.2, ОПК-5.3, ПК-4, ПК-5, ПК-6	0,2	5	4	3	2
4. Степень самостоятельности исследования	УК-3, УК-6, ОПК-2, ОПК-10, ОПК-11, ОПК-16, ОПК-5.1 ПК-4, ПК-5	0,2	5	4	3	2
5. Навыки публичной дискуссии, защиты собственных научных идей, предложений и рекомендаций	УК-4, УК-8, ОПК-4, ОПК-17 ПК-1, ПК-2	0,1	5	4	3	2

6. Общий уровень культуры общения с аудиторией	УК-5, УК-7, УК-9, УК-10, ОПК-1, ОПК-17 ПК-2, ПК-5	0,1	5	4	3	2
7. Полнота и точность ответов на вопросы	УК-1, ОПК-1, ОПК-14, ОПК-15, ОПК-16, ОПК-17 ПК-2, ПК-3	0,1	5	4	3	2

Каждый критерий оценивается по 5-балльной шкале. Оценка результата ВКР выполняется с использованием формулы:

$P = \sum_{i=1}^n P_i * k_i,$
где $P_i$ – оценка каждого критерия ВКР, в баллах; $k_i$ – удельный вес каждого критерия; $P$ – округляется до целого в большую сторону.

Результаты защиты ВКР определяются оценками: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Шкала интерпретации результатов оценивания компетенций и критерии оценки результатов защиты ВКР приведена в таблице 3.

Таблица 3. Шкала интерпретации результатов оценивания компетенций на защите ВКР

Итоговый результат (P)	Критерии оценки результатов защиты ВКР	Оценка результатов защиты ВКР и ГИА
2	Уровень владения компетенциями для решения профессиональных задач недостаточен: значительная часть результатов выполнения ВКР, ответы на вопросы членов ГЭК содержат ошибки, характер которых указывает на недостаточный уровень владения выпускником знаниями, умениями, навыками и (или) опытом, необходимыми для решения профессиональных задач.	Неудовлетворительно
3	Уровень владения компетенциями для решения профессиональных задач удовлетворителен: некоторые результаты выполнения ВКР, ответы на вопросы членов ГЭК содержат ошибки, характер которых указывает на посредственный уровень владения выпускником необходимыми знаниями, умениями, навыками и (или) опытом, но при этом позволяет сделать вывод о готовности выпускника решать типовые профессиональные задачи в стандартных ситуациях.	Удовлетворительно
4	Уровень владения компетенциями для решения профессиональных задач преимущественно высокий: некоторые результаты выполнения ВКР, ответы на вопросы членов ГЭК содержат незначительные ошибки и технические погрешности, характер которых указывает на преимущественно высокий уровень владения выпускником необходимыми знаниями, умениями, навыками и (или) опытом и позволяет сделать вывод о готовности выпускника решать типовые и ситуативные профессиональные задачи.	Хорошо
5	Уровень владения компетенциями для решения профессиональных задач высокий:	Отлично

Итоговый результат (P)	Критерии оценки результатов защиты ВКР	Оценка результатов защиты ВКР и ГИА
	результаты выполнения ВКР, ответы на вопросы членов ГЭК не содержат ошибок и технических погрешностей, указывают на высокий уровень владения выпускником необходимыми знаниями, умениями, навыками и (или) опытом и позволяют сделать вывод о готовности выпускника решать профессиональные задачи повышенного уровня сложности, а также способности разрабатывать новые решения.	

### 3. ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ ИЛИ ИНЫЕ МАТЕРИАЛЫ, НЕОБХОДИМЫЕ ДЛЯ ОЦЕНКИ РЕЗУЛЬТАТОВ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

#### 3.1 Типовые контрольные задания или иные материалы, необходимые для оценки результатов освоения образовательной программы, на защите ВКР

##### 3.1.1 Примерный перечень тем ВКР

1. Аудит и подготовка к аттестации информационной системы обработки персональных данных предприятия.
2. Разработка комплекса средств обеспечения сетевой безопасности на территориально распределенных объектах организации.
3. Разработка системы защиты от несанкционированного доступа к информационным ресурсам промышленного предприятия.
4. Разработка и исследование методов встраивания цифровых водяных знаков в файлы растровых графических данных, циркулирующие в распределенной автоматизированной системе.
5. Разработка и исследование методов стеганоанализа цифровой видеоинформации.
6. Разработка и исследование методов многофакторной аутентификации пользователя распределенной информационной системы.
7. Разработка системы автоматизированной проверки подлинности программных средств защиты информации.
8. Разработка системы автоматизации обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные системы.
9. Разработка алгоритмов и программных средств детектирования сетевых аномалий методами машинного обучения.
10. Разработка и исследование методов защиты информационных систем от массовых автоматически генерируемых клиентских запросов.
11. Исследование алгоритмов и программных средств противодействия атаке "человек посередине" на распределенную автоматизированную систему.
12. Разработка и исследование методов повышения защищенности протоколов аутентификации "3D Secure" от атак, основанных на применении вредоносного клиентского программного обеспечения.
13. Использование технологии blockchain для безопасного взаимодействия объектов в распределенной информационной системе.
14. Разработка и исследование метода обнаружения подделок скан-копий документов
15. Разработка утилиты сбора информации и предварительного анализа защищенности веб-приложения
16. Метод защиты авторских прав на изображения на основе нейросетевого подхода
17. Реализация алгоритма стеганографического встраивания информации в текстовые данные

18. Разработка анонимизирующего мессенджера на основе криптографических методов защиты информации
19. Разработка и программная реализация протокола взаимной аутентификации с использованием одноразовых паролей и QR кодов
20. Разработка и исследование методов обнаружения атак на биометрическое предъявление
21. Разработка и исследование нейросетевого метода обнаружения следов подделки цифровых изображений
22. Разработка метода защиты от атак на нейронные обработки данных
23. Разработка и реализация стойких алгоритмов выработки криптографических ключей
24. Разработка и исследование методов биометрической идентификации личности
25. Разработка системы контроля и управления доступом с применением технологии распознавания лиц
26. Обнаружение SQL-инъекций в HTTP-запросах
27. Разработка защищенной системы онлайн голосования на основе технологии блокчейн
28. Разработка и исследование алгоритмов анализа подлинности и выявления признаков монтажа цифровых видеозаписей
29. Обнаружение фальсифицированных цифровых аудиозаписей на основе анализа фоновых шумов
30. Повышение безопасности передачи информации, осуществляемой по технологии OFDM
31. Разработка системы обнаружения аномального поведения пользователя ЭВМ
32. Повышение защищенности сетевых взаимодействий в кластере Kubernetes
33. Разработка и исследование методов обнаружения ботов в социальных сетях
34. Построение системы защиты ИСПДн удостоверяющего центра
35. Исследование канала утечки информативных сигналов за счет наводок на линии электропитания и передачи данных

### 3.1.2. Перечень примерных вопросов на защите ВКР

Таблица 4. Перечень примерных вопросов на защите ВКР

Код и наименование проверяемой компетенции	Примерные вопросы
Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, выработать стратегию действий (УК-1)	К каким общим закономерностям относятся процессы, выявленные вами в ходе анализа предмета ВКР? Какие из разработанных в ВКР рекомендаций могут носить универсальный характер, использоваться при анализе других объектов?
Способен управлять проектом на всех этапах его жизненного цикла (УК-2)	Охарактеризуйте основные этапы проведенного исследования. Какие направления выполненного исследования могут получить дальнейшее развитие?
Способен организовывать и руководить работой команды, выработывая командную стратегию для достижения поставленной цели (УК-3)	Какой коллектив участников необходим для реализации проекта внедрения Вашей ВКР? Каким образом распределить обязанности и организовать взаимодействие между членами команды?
Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия (УК-4)	Какие зарубежные научные издания являются ведущими по выбранной Вами теме ВКР? Какие из источников на иностранных языках изучены в ходе подготовки ВКР?

<p>Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия (УК-5)</p>	<p>Принимали ли Вы участие в научных семинарах с представителями различных культур?          Каким образом организовать взаимодействие внутри команды в ходе реализации проекта с учетом разнообразия культур?</p>
<p>Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни (УК-6)</p>	<p>Как вы расставляли приоритеты в собственной работе над ВКР?          Какие новые компетенции Вы приобрели, работая над ВКР?</p>
<p>Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности (УК-7)</p>	<p>Знакомы ли Вы со способами организации режима труда и отдыха? Использовали ли Вы их при подготовке выпускной квалификационной работы?</p>
<p>Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов (УК-8)</p>	<p>Знакомы ли Вы с правилами техники безопасности при работе с вычислительной техникой? Соблюдали ли Вы их при работе над ВКР?          Что называется опасной зоной?</p>
<p>Способен принимать обоснованные экономические решения в различных областях жизнедеятельности (УК-9)</p>	<p>Как оценить экономическую эффективность от внедрения Вашей ВКР?          В чем состоят основные затраты на разработку и внедрение защищенных автоматизированных систем?</p>
<p>Способен формировать нетерпимое отношение к коррупционному поведению (УК-10)</p>	<p>Что такое противодействие коррупции?          Встречались ли Вы во время обучения в университете и при подготовке ВКР с проявлениями коррупционного поведения?</p>
<p>Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства (ОПК-1)</p>	<p>Выделите основные проблемы информационной безопасности. Каково значение информационных технологий в современном обществе?          Оцените важность вопроса обеспечения информационной безопасности для государства.</p>
<p>Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности (ОПК-2)</p>	<p>Какие программные средства применялись при анализе защищенности автоматизированной системы?          Как проводилась проверка работоспособности примененных вами программных средств системного и прикладного назначений?</p>
<p>Способен использовать математические методы, необходимые для решения задач профессиональной деятельности (ОПК-3)</p>	<p>Какие методы математического анализа, алгебры, дискретной математики, теории чисел были использованы в ВКР?          Какие методы теории вероятностей, математической статистики применялись в работе над ВКР?</p>

<p>Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности (ОПК-4)</p>	<p>Какие законы классических и квантовых физических явлений и процессов были использованы при исследовании защищенности объекта, рассматриваемого в ВКР?</p>
<p>Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации (ОПК-5)</p>	<p>Укажите нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа, которые были учтены при вводе в эксплуатацию объекта информатизации, предложенного в ВКР? Какими электронными ресурсами, содержащими базы нормативных документов по информационной безопасности Вы пользовались при выполнении ВКР?</p>
<p>Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю (ОПК-6)</p>	<p>Выполните классификацию защищаемой информации по видам тайн С информацией каких степеней классификации вы работали в процессе выполнения ВКР? Произведите оценку угроз информационной безопасности для объекта информатизации, рассматриваемого в ВКР</p>
<p>Способен создавать программы на языках общего назначения, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ (ОПК-7)</p>	<p>Какие языки и системы программирования, инструментальные средства были использованы для решения прикладных задач в ВКР? Проходили ли тестирование и отладку программные средства, разработанные в ВКР?</p>
<p>Способен применять методы научных исследований при проведении разработок в области защиты информации в автоматизированных системах (ОПК-8)</p>	<p>Какие физические и математические методы были использованы при выполнении экспериментальных исследований в ходе выполнения ВКР? Какие технические и программные средства были использованы при выполнении экспериментальных исследований в ходе выполнения ВКР?</p>
<p>Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации (ОПК-9)</p>	<p>Насколько вы учли современные тенденции развития информатики и вычислительной техники, компьютерных технологий в ВКР при выборе программных средств и сетевой конфигурации? Какие новейшие программные средства были использованы при выполнении ВКР?</p>

<p>Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности (ОПК-10)</p>	<p>Как проводилась проверка работоспособности примененных вами технических средств защиты информации?          Как проводилась проверка работоспособности примененных вами криптографических средств защиты информации?          Как проводилась проверка работоспособности примененных вами программно-аппаратных средств защиты информации?</p>
<p>Способен разрабатывать компоненты систем защиты информации автоматизированных систем (ОПК-11)</p>	<p>В разработке каких средств защиты информации автоматизированных систем Вы участвовали в ходе выполнения ВКР?</p>
<p>Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем (ОПК-12)</p>	<p>Производилась ли оценка рисков информационной безопасности операционных систем и баз данных, применяемых в ВКР?</p>
<p>Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем (ОПК-13)</p>	<p>Когда возникает необходимость аудита информационной безопасности распределенной информационной системы?          Чем регламентируется проведение аудита информационной безопасности распределенной информационной системы?</p>
<p>Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений (ОПК-14)</p>	<p>Была ли разработана политика управления доступом и информационными потоками в компьютерных системах, исследуемых в ВКР?          Какими способами моделирования безопасности компьютерных систем вы овладели в ходе выполнения ВКР?</p>
<p>Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем (ОПК-15)</p>	<p>Сформулируйте основные требования информационной безопасности при эксплуатации компьютерной системы и технических средств защиты информации, рассматриваемых в ВКР?          Был ли проведен анализа безопасности компьютерных систем, рассматриваемых в ВКР, на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности систем и средств обеспечения информационной безопасности?</p>
<p>Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма (ОПК-16)</p>	<p>Какие исторически закономерные процессы выделены вами в функционировании вашего объекта?          К каким общим закономерностям относятся процессы, выявленные вами в ходе анализа предмета ВКР?          Какие из полученных вами выводов ВКР могут быть полезны для других объектов?</p>

<p>Способен разрабатывать и реализовывать политику информационной безопасности открытых информационных систем (ОПК-5.1)</p>	<p>Какими нормативными документами регламентируется разработка политики информационной безопасности автоматизированной системы? Какие основные аспекты защиты информации необходимо учитывать при разработке политики информационной безопасности автоматизированной системы?</p>
<p>Способен разрабатывать и эксплуатировать системы защиты информации открытых информационных систем (ОПК-5.2)</p>	<p>Как организовать внедрение открытой информационной системы с учетом требований информационной безопасности? Как организовать эксплуатацию и сопровождение открытой информационной системы с учетом требований информационной безопасности?</p>
<p>Способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах (ОПК-5.3)</p>	<p>Как осуществлялся контроль обеспечения информационной безопасности в открытых информационных системах, использованных в ВКР? Как проводилась верификация данных при выполнении ВКР?</p>
<p>Способен выполнять интеграцию программных модулей и компонент, проводить верификацию программных продуктов (ПК-1)</p>	<p>Осуществлялась ли интеграция программных модулей и компонент в процессе выполнения ВКР? Проводилась ли верификация программных продуктов при выполнении ВКР?</p>
<p>Способен разрабатывать требования и проектировать программное обеспечение (ПК-2)</p>	<p>Какие требования ставились Вами к разработанному в ВКР программному обеспечению? Какие парадигмы и методы проектирования программного обеспечения использованы в ВКР?</p>
<p>Способен разрабатывать системные утилиты и компоненты операционной системы (ПК-3)</p>	<p>Какие системные утилиты и компоненты операционной системы были разработаны при выполнении ВКР? Чем отличаются системные утилиты и компоненты операционной системы?</p>
<p>Способен разрабатывать системы защиты информации автоматизированных систем (ПК-4)</p>	<p>Какие Вы знаете средства разработки систем защиты автоматизированных систем? Какие из них использовались в ВКР?</p>
<p>Способен осуществлять непосредственное руководство процессами разработки программного обеспечения (ПК-5)</p>	<p>Как организовать разработку автоматизированной системы Как осуществлять руководство разработкой с учетом требований информационной безопасности?</p>
<p>Способен оценивать уровень безопасности компьютерных систем и сетей (ПК-6)</p>	<p>Какие факторы и параметры необходимо учитывать при оценке уровня безопасности компьютерных систем и сетей? Как оценивался уровень безопасности системы, разработанной в рамках ВКР?</p>

Способен применять методы анализа данных для решения задач информационной безопасности (ПК-7)	Какие методы машинного обучения и статистического анализа данных Вам известны? Какие методы анализа данных использовались при выполнении ВКР?
Способен разрабатывать и использовать методы защиты данных, хранящихся и передаваемых в автоматизированных системах (ПК-8)	Осуществлялась ли специализированная защита данных, использованных в рамках ВКР? Выделите основные классы методов защиты данных, хранящихся и передаваемых в автоматизированных системах.

#### 4. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Защита ВКР является завершающим этапом и ГИА. Не позднее, чем за 2 календарных дня до защиты ВКР обучающийся представляет секретарю ГЭК ВКР, отзыв руководителя и рецензию на ВКР.

Специалист института за 2 рабочих дня до защиты ВКР передает секретарю ГЭК следующие документы:

- приказ об утверждении составов ГЭК для проведения ГИА и апелляционных комиссий по результатам ГИА (копия);
- распоряжение директора института об утверждении расписания государственных аттестационных испытаний (копия);
- приказ об утверждении тем и руководителей ВКР (копия);
- программу ГИА (копия);
- распоряжение директора института о допуске обучающихся к ГИА (копия);
- заявления от обучающихся из числа инвалидов о необходимости (отсутствие необходимости) присутствия ассистента на государственном аттестационном испытании, о необходимости (отсутствие необходимости) увеличения продолжительности сдачи государственного аттестационного испытания по отношению к установленной продолжительности (для каждого государственного аттестационного испытания (копии, при наличии));
- проект приложения к диплому, согласованный с выпускником, списки выпускников, претендующих на получение диплома с отличием;
- списки выпускников, распределенные по дням защиты ВКР в соответствии с расписанием ГИА;
- экзаменационные ведомости по приему государственного аттестационного испытания.

На основании представленных документов секретарь ГЭК готовит:

- бланки оценочных листов каждому члену ГЭК;
- протоколы заседания ГЭК по защите ВКР на каждый день защиты ВКР согласно расписанию ГИА.

Защита ВКР проводится в виде открытых заседаний ГЭК с участием не менее двух третей ее списочного состава.

Заседания ГЭК по защите ВКР проводится согласно утвержденному расписанию ГИА.

Процедура защиты ВКР включает в себя:

–открытие заседания ГЭК: председатель ГЭК в начале заседания излагает порядок защиты, принятия решения, оглашения результатов ГЭК; устанавливает обучающимся время для устного изложения основных результатов ВКР и ответов на вопросы членов ГЭК;

–доклад выпускника: доклад должен сопровождаться показом презентации, выполненной в редакторе Microsoft PowerPoint или его аналогах с иллюстрациями, таблицами, рисунками, схемами и пояснениями и распечатанной на бумажном носителе в качестве раздаточного материала для каждого члена ГЭК;

–вопросы членов ГЭК (записываются в протокол заседания ГЭК);

–заслушивание отзыва: после ответа обучающегося на все вопросы отзыв руководителя зачитывает секретарь ГЭК, при отсутствии отзыва требуется личное присутствие и выступление руководителя ВКР с отзывом;

–заслушивание рецензии: секретарь ГЭК зачитывает письменный отзыв рецензента;

–заключительное слово обучающегося: обучающемуся предоставляется возможность ответить на замечания, сделанные рецензентом;

–продолжительность выступления обучающегося при защите ВКР – не более 10 минут, ответы на вопросы членов комиссии – не более 10 минут. Общая продолжительность процедуры защиты ВКР обучающегося – не более 30 минут.

Члены ГЭК на закрытом заседании оценивают результаты защиты ВКР каждым обучающимся и результаты освоения образовательной программы. Решения ГЭК принимаются на основе открытого голосования простым большинством голосов от числа лиц, входящих в состав ГЭК и участвующих в заседании. При равном числе голосов председатель ГЭК обладает правом решающего голоса.

Результаты защиты ВКР определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Оценки «отлично», «хорошо», «удовлетворительно» означают успешное ГИА.

Результаты защит ВКР оглашает председатель ГЭК после окончания закрытой части заседания ГЭК в день его проведения.

Оценка за защиту ВКР проставляется в зачетную книжку обучающегося, в экзаменационную ведомость по защите ВКР и в протокол заседания ГЭК по защите ВКР. Оценка за защиту ВКР, проставленная в зачетную книжку обучающегося и в экзаменационную ведомость по защите ВКР подтверждается подписями председателя и секретаря ГЭК. Протокол заседания ГЭК по защите ВКР подписывают председатель и секретарь ГЭК

По окончании всех заседаний ГЭК по защите ВКР протоколы заседаний ГЭК сшиваются в книги. Книги передаются для хранения в архив университета, остальные документы передаются секретарем ГЭК специалисту института для организации хранения в институте.

Обучающиеся, не прошедшие защиту ВКР в связи с неявкой на данное государственное аттестационное испытание по неуважительной причине или в связи с получением оценки «неудовлетворительно», а также обучающиеся из числа инвалидов, не прошедшие данное государственное аттестационное испытание в установленный для них срок (в связи с неявкой на данное государственное аттестационное испытание или получением оценки «неудовлетворительно»), отчисляются из университета с выдачей справки об обучении как не выполнившие обязанностей по добросовестному освоению образовательной программы и выполнению учебного плана по установленной форме.

ФОС для проведения ГИА обсужден на заседании кафедры геоинформатики и информационной безопасности

Протокол № 4 от «17» марта 2021 г.

Заведующий кафедрой геоинформатики  
и информационной безопасности

\_\_\_\_\_ /В.В. Сергеев /