

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Грובה Татьяна Анатольевна

Должность: и.о. декана факультета математики и компьютерных наук имени
профессора Н.И. Червякова

Дата подписания: 17.06.2026 16:08:19

Уникальный программный ключ:

bd39d4208aa94cf4422feb787c81619d42de79a7

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования

«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

Декан факультета математики и
компьютерных наук имени
профессора Н.И.Червякова
_____ Т. А. Грובה

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

Направление подготовки	10.04.01 Информационная безопасность
Направленность (профиль)/специализация	Информационная безопасность киберфизических систем
Год начала обучения	2026
Форма обучения	очная
Реализуется в семестре	4

СОГЛАСОВАНО:

Представитель работодателя
Директор ООО «Инфоком С»
_____ Н.Г. Демурчев

РАЗРАБОТАНО:

Доцент кафедры организации и технологии
защиты информации
Бисюков Виктор Михайлович

Рассмотрено УМК факультета математики и
компьютерных наук имени профессора
Н.И.Червякова
№ __ от __ _____ 2026 г.

Ставрополь, 2026

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

Декан факультета математики и
компьютерных наук имени
профессора Н.И. Червякова
_____ Т. А. Грובה

**ПРОГРАММА
ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ**

Направление подготовки	<u>10.04.01 Информационная безопасность</u>
Направленность (профиль)/специализация	<u>Информационная безопасность киберфизических систем</u>
Год начала обучения	<u>2026</u>
Форма обучения	<u>очная</u>
Реализуется в семестре	<u>4</u>

РАЗРАБОТАНО:

Доцент кафедры организации и технологии
защиты информации
Бисюков Виктор Михайлович

Ставрополь, 2026

Введение

1. Состав итоговой (государственной итоговой) аттестации

В соответствии с ФГОС по направлению подготовки 10.04.01 «Информационная безопасность», утверждённым Приказ №1455 от 26.11.2020 и образовательной программой по направлению подготовки 10.04.01 «Информационная безопасность», утвержденной Учёным советом СКФУ в государственную итоговую аттестацию входят:

- подготовка к сдаче и сдача государственного экзамена по направлению подготовки 10.04.01 «Информационная безопасность»,
- выполнение и защита выпускной квалификационной работы.

2. Программа ГИА составлена в соответствии с требованиями:

- ФГОС по направлению подготовки 10.04.01 «Информационная безопасность», утверждённым министерством образования и науки РФ. Приказ №1455 от 26.11.2020,
- образовательной программы высшего образования по направлению подготовки 10.04.01 «Информационная безопасность», утвержденной Учёным советом СКФУ,
- Положения о порядке проведения государственной итоговой аттестации обучающихся по образовательным программам высшего образования – программам бакалавриата, программам специалитета и программам магистратуры в ФГАОУ ВО «Северо-Кавказский федеральный университет», принято УС СКФУ протокол от 26.10.2017 № 3, в редакции от 27.12.2018 г., протокол УС СКФУ № 7.
- Положения о порядке выполнения выпускных квалификационных работ в федеральном государственном автономном образовательном учреждении высшего образования «Северо-Кавказский федеральный университет», принято УС СКФУ протокол от 30.01.2018 № 7
- Положения об учебно-методическом обеспечении образовательных программ высшего образования в ФГАОУ ВО «Северо-Кавказский федеральный университет», утверждено решением Ученого совета СКФУ протокол № 12 от 20 февраля 2023 г.

3. Компетенции, которыми должен овладеть обучающийся в результате освоения образовательной программы высшего образования

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
ОПК-1	Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание
ОПК-2	Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности

ОПК-3	Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности
ОПК-4	Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок
ОПК-5	Способен проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи
ПК-1	Способен проводить исследования и анализ информационных процессов защиты информации в киберфизических системах
ПК-2	Способен проектировать и реализовывать политику безопасности вычислительных сетей в киберфизических системах
ПК-3	Способен разрабатывать предложения по совершенствованию системы управления информационной безопасностью киберфизических систем
ПК-4	Способен оценивать уровень защищенности киберфизических систем и применять решения по обеспечению их информационной безопасности

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

Декан факультета математики и
компьютерных наук имени
профессора Н.И. Червякова
_____ Т. А. Грובה

**ПРОГРАММА
ГОСУДАРСТВЕННОГО ЭКЗАМЕНА**

Направление подготовки	10.04.01 Информационная безопасность
Направленность (профиль)/специализация	Информационная безопасность киберфизических систем
Год начала обучения	2026
Форма обучения	очная
Реализуется в семестре	4

РАЗРАБОТАНО:

Доцент кафедры организации и технологии
защиты информации
Бисюков Виктор Михайлович

Ставрополь, 2026

1. Цели и задачи государственного экзамена

Заключительный этап теоретического обучения магистра в высшем учебном заведении состоит в подготовке и сдаче государственного экзамена. Государственный экзамен по направлению 10.04.01 «Информационная безопасность» преследует цель провести оценку степени профессиональной подготовки выпускника по использованию теоретических знаний, практических навыков и умений для решения профессиональных задач в области информационной безопасности на уровне, требуемом ФГОС ВПО по направлению 10.04.01 «Информационная безопасность» с учетом специфики учебного процесса и региональных особенностей вуза.

Государственный экзамен по направлению 10.04.01 «Информационная безопасность» проводится в форме итогового экзамена.

Основными задачами государственного экзамена являются:

- определение соответствия подготовки студента выпускного курса СКФУ требованиям ФГОС ВО по направлению 10.04.01 «Информационная безопасность» и уровня его подготовки

- принятие решения о присвоении квалификации (степени) по результатам государственной итоговой аттестации и выдаче выпускнику Университета соответствующего диплома государственного образца о высшем профессиональном образовании

- разработка рекомендаций, направленных на совершенствование качества подготовки специалистов, на основании результатов работы государственной аттестационной комиссии.

2. Перечень компетенций, уровень сформированности которых должен быть проверен на государственном экзамене

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
ОПК-1	Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание
ОПК-2	Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности
ОПК-3	Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности
ОПК-4	Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок

ОПК-5	Способен проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи
-------	--

3. Структура государственного экзамена

Государственный экзамен имеет междисциплинарный характер и включает вопросы по следующим дисциплинам учебного плана подготовки магистров направления 10.04.01 «Информационная безопасность»:

1. Управление информационной безопасностью.
2. Технологии обеспечения информационной безопасности
3. Защищённые информационные системы.
4. Методология научных исследований.

Экзамен предполагает:

1. Ответ экзаменуемого по теоретическим вопросам.
2. Практическое выполнение задания.

Структурно экзаменационный билет состоит из 3 заданий, соответствующих 3 различным дисциплинам. Каждый билет содержит 2 теоретических вопроса (базовый уровень) и практический вопрос (повышенный уровень).

4. Содержание государственного экзамена

Программа междисциплинарного государственного экзамена по направлению 10.04.01 «Информационная безопасность» включает основополагающие темы следующих учебных дисциплин:

Управление информационной безопасностью

Основы управления информационной безопасностью. Система управления информационной безопасностью. Основы управления рисками информационной безопасности. Процессы управления информационной безопасности.

Технологии обеспечения информационной безопасности

Значение информационной безопасности и ее место в системе национальной безопасности. Сущность и понятие защиты информации. Теоретические и концептуальные основы защиты информации объектов. Критерии, условия и принципы отнесения информации к защищаемой. Состав и классификация носителей защищаемой информации. Источники, виды и способы дестабилизирующего воздействия на защищаемую информацию. Каналы и методы несанкционированного доступа к конфиденциальной информации. Объекты защиты информации. Классификация видов, методов и средств защиты информации. Кадровое и ресурсное обеспечение защиты информации. Технологическое обеспечение защиты информации на объекте. Структура систем защиты информации объекта. Аудит информационной безопасности объекта.

Защищённые информационные системы

Механизмы защиты операционной системы. Интеграция защищенных операционных систем. Типовые угрозы сетевой безопасности. Методы и средства обеспечения информационной безопасности в вычислительных сетях. Теоретические основы

безопасности в СУБД. Механизмы обеспечения конфиденциальности, целостности и высокой готовности СУБД.

Методология научных исследований

Научное исследование, его сущность и организация. Структура научного знания. Основы методологии научных исследований. Общая характеристика метода и методологии научного исследования. Основные этапы планирования и проведения научного исследования. Источники научной информации. Методика работы с источниками научной информации. Оформление и защита научных работ. Методика работы над рукописью исследования. Особенности презентации и защиты результатов исследования.

5. Перечень примерных вопросов для подготовки к государственному экзамену

5.1 Теоретические вопросы к государственному экзамену:

I. Управление информационной безопасностью:

1. Основы управления информационной безопасностью
2. Система управления информационной безопасностью
3. Основы управления рисками информационной безопасности
4. Процессы управления информационной безопасности.

II. Технологии обеспечения информационной безопасности:

1. Значение информационной безопасности и ее место в системе национальной безопасности
2. Сущность и понятие защиты информации
3. Теоретические и концептуальные основы защиты информации объектов
4. Критерии, условия и принципы отнесения информации к защищаемой
5. Состав и классификация носителей защищаемой информации
6. Источники, виды и способы дестабилизирующего воздействия на защищаемую информацию.
7. Каналы и методы несанкционированного доступа к конфиденциальной информации
8. Объекты защиты информации
9. Классификация видов, методов и средств защиты информации
10. Кадровое и ресурсное обеспечение защиты информации
11. Технологическое обеспечение защиты информации на объекте
12. Структура систем защиты информации объекта
13. Аудит информационной безопасности объекта.

III. Защищённые информационные системы

1. Механизмы защиты операционной системы
2. Интеграция защищенных операционных систем
3. Типовые угрозы сетевой безопасности
4. Методы и средства обеспечения информационной безопасности в вычислительных сетях
5. Теоретические основы безопасности в СУБД
6. Механизмы обеспечения конфиденциальности, целостности и высокой готовности

IV. Методология научных исследований

1. Научное исследование, его сущность и организация
2. Структура научного знания
3. Основы методологии научных исследований
4. Общая характеристика метода и методологии научного исследования
5. Основные этапы планирования и проведения научного исследования
6. Источники научной информации
7. Методика работы с источниками научной информации
8. Оформление и защита научных работ
9. Методика работы над рукописью исследования
10. Особенности презентации и защиты результатов исследования.

5.2 Практические вопросы к государственному экзамену:

1. Обнаружить и локализовать радиозакладные устройства в помещении детектором поля ST-107 в режиме поиска.
2. Обнаружить и локализовать радиозакладные устройства в помещении детектором поля ST-107 в режиме мониторинга.
3. Обнаружить закладные устройства в линии 220В помещения прибором ST-033 «Пиранья». в режиме анализатора проводных линий .
4. Обнаружить и локализовать радио закладные устройства в телефонной линии помещения прибором ST-107.
5. Продемонстрировать инфракрасный канал утечки информации в помещении прибором ST-033 «Пиранья».
6. Продемонстрировать акустический канал утечки информации помещении прибором ST-033 «Пиранья».
7. Продемонстрировать вибро-акустический канал утечки информации в помещении прибором ST-033 «Пиранья».
8. Обнаружить телефонные радио ретрансляторы на учебной телефонной линии нелинейным радиолокатором «Лорнет».
9. Обнаружить радиозакладные устройства в помещении специальным сканирующим приёмником «Скорпион».
10. Заблокировать канал утечки информации по системам цифровой связи с использованием прибора «Квартет-2».
11. Заблокировать канал утечки информации по системам цифровой связи с использованием прибора «Филин-4».
12. Обнаружить любым прибором и заблокировать радиоканалы утечки информации широкополосным генератором шума «Штора-4».
13. Обнаружить и заблокировать радиоканал утечки информации в помещении специальным сканирующим приёмником «Скорпион».
14. Обнаружить радиоканал утечки информации в помещении с использованием прибора ST-033 «Пиранья».
15. Обнаружить телефонный радиоретранслятор на учебной телефонной линии нелинейным радиолокатором НРЛ «NRL-900 EMS»
16. Провести обследование помещения на предмет наличия закладных устройств НРЛ

«Лорнет».

17. Провести обследование помещения на предмет наличия закладных устройств НРЛ «NRL-900 EMS»

18. Продемонстрировать защиту от утечек информации по каналу ПЭМИ в помещении с использованием прибора «Соната-РК»

19. Обнаружить радио канал утечки информации сканирующим приемником AR-8600

20. Продемонстрировать работу микрофонной и телефонной радиозакладки с использованием сканирующего приемника «Скорпион»

21. Обнаружить сигнал микрофонной закладки в помещении с использованием ПАК «Кассандра К-21».

22. Обнаружить сигнал ТЛФ закладки в помещении с использованием ПАК «Кассандра К-21».

23. Обнаружить сигналы сотовых систем связи с использованием ПАК «Кассандра К-21»

24. Продемонстрировать обнаружение радиосигналов с использованием режима «Водопад»

25. Обнаружить работу радиовидеокамеры сканирующим приемником «Скорпион» в панорамном режиме.

26. Обнаружить сигнал радиовидеокамеры ПАК «Кассандра К-21»

27. Обнаружить и локализовать ТЛФ радиоретранслятор с использованием прибора «Пиранья» ST-033

6. Список рекомендуемой литературы

6.1. Основная литература

1. Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность: учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва: Издательство Юрайт, 2022. — 473 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/489242> (дата обращения: 18.10.2022).

2. Технические средства и методы защиты информации: учебное пособие / А. П. Зайцев, А. А. Шелупанов, Р. В. Мещеряков, И. В. Голубятников. — Москва: Горячая линия-Телеком, 2012. — 616 с. — ISBN 978-5-9912-0084-4. — Текст: электронный // Лань: электронно-библиотечная система. — URL: <https://e.lanbook.com/book/5154> (дата обращения: 18.10.2022).

3. Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3 т. Том 1. Технические каналы утечки информации. - М.: НПЦ «Аналитика», 2008. - 436 с.: ил

4. Петренко В. И., Ванина А. Г., Минкина Т. В. Патентоведение: учебное пособие (курс лекций). – Ставрополь: Изд-во СКФУ, 2020. – 116 с.

5. Петренко В. И. Теоретические основы защиты информации: учебное пособие. – Ставрополь: Изд-во СКФУ, 2015. – 222 с.

6.2 Дополнительная литература:

1. Костромитин, К. И. Инженерно-техническая защита информации и технические средства охраны на критически важных объектах: учебное пособие / К. И. Костромитин. — Москва: Ай Пи Ар Медиа, 2022. — 137 с. — ISBN 978-5-4497-1765-8. — Текст: электронный

// Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/122647.html> (дата обращения: 23.09.2022).

2. Креопалов, В.В. Технические средства и методы защиты информации: учебно-практическое пособие / В.В. Креопалов. - М.: Евразийский открытый институт, 2011. - 278 с.

3. Куприянов, А. И. Исследование криптографических методов защиты информации: учебное пособие / А. И. Куприянов, В. Ф. Макаров. — Москва: Московский государственный технический университет имени Н.Э. Баумана, 2019. — 110 с. — ISBN 978-5-7038-5059-6. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/110633.html> (дата обращения: 18.10.2022).

4. Леонтьев, А. С. Защита информации: учебное пособие / А. С. Леонтьев. — Москва: РТУ МИРЭА, 2021. — 79 с. — Текст: электронный // Лань: электронно-библиотечная система. — URL: <https://e.lanbook.com/book/182491> (дата обращения: 18.10.2022). — Режим доступа: для авториз. пользователей.

7. Организация и проведение государственного экзамена

Целью государственного экзамена является оценка степени профессиональной подготовки выпускника по использованию теоретических знаний, практических навыков и умений, уровня сформированности компетенций для решения профессиональных задач на уровне, требуемом стандартом.

Для работы экзаменационной комиссии секретарь государственной экзаменационной комиссии представляет следующие документы: копию приказа ректора СКФУ о допуске студентов к ГИА, справки о выполнении учебного плана по каждому студенту, допущенному к ГИА в соответствии с приказом о допуске, экзаменационные ведомости о сдаче государственного экзамена, форму оценки членами ГЭК уровня сформированности компетенций в ходе государственного экзамена (Оценочный лист).

Перед началом государственного экзамена председателем государственной экзаменационной комиссии или по его распоряжению членом государственной экзаменационной комиссии раскладываются экзаменационные билеты.

При сдаче государственного экзамена в устной форме допускается присутствие в аудитории не более 7 студентов. Каждый студент самостоятельно выбирает экзаменационный билет один раз посредством произвольного извлечения. Номер билета фиксируется секретарем ГЭК в соответствующем протоколе.

На подготовку к ответу на экзаменационный билет студенту отводится 1 час. При подготовке студент имеет право пользоваться программой государственного экзамена, а также с разрешения ГЭК - справочной литературой.

Студенты, использующие при подготовке к ответу другую учебную литературу, средства связи и электронно-вычислительную технику (кроме калькулятора), с государственного экзамена удаляются. В протоколе после слов «Признать, что студент сдал государственный экзамен с оценкой» заносится запись «неудовлетворительно. Студент удален с государственного экзамена за нарушение порядка проведения государственного экзамена». В экзаменационной ведомости студенту также проставляется оценка «неудовлетворительно».

При оценке ответа студента на государственном экзамене учитывается уровень сформированности компетенций, другие требования, предъявляемые фондом оценочных средств для проведения государственной итоговой аттестации, разработанным выпускающей

кафедрой по каждой образовательной программе.

По окончании ответа студента председатель и члены комиссии могут задавать дополнительные вопросы (как правило, не более трех). Секретарь комиссии вносит в протокол задания билета, дополнительные вопросы членов комиссии, а также общую характеристику ответа студента на все вопросы.

В целом ответ студента на экзаменационный билет и дополнительные вопросы занимает, как правило, 30 минут.

В случае если студент по состоянию здоровья не смог ответить на задания экзаменационного билета, в протокол после слов «Общая характеристика ответа...» вносится запись «Студент по состоянию здоровья не смог ответить на задания экзаменационного билета». Факт болезни должен быть подтвержден заключением медицинских работников. Срок повторной сдачи государственного экзамена назначается дополнительно.

По окончании ответов студентов академической группы объявляется совещание экзаменационной комиссии, на котором присутствуют только члены комиссии. На совещании обсуждаются ответы каждого студента на задания билета и дополнительные вопросы.

По итогам обсуждения каждому студенту в протокол проставляется соответствующая оценка. Секретарь комиссии заполняет экзаменационную ведомость по итогам проведения государственного экзамена.

После совещания комиссии в аудиторию приглашаются студенты академической группы. Председатель комиссии информирует студентов о результатах государственного экзамена.

8. Описание показателей и критериев оценивания компетенций, а также шкал оценивания

8.1 Описание показателей

Уровни сформированности компетенции (ий), индикатора (ов)	Дескрипторы			
	Минимальный уровень не достигнут (неудовлетворительно) 2 балла	Минимальный уровень (удовлетворительно) 3 балла	Средний уровень (хорошо) 4 балла	Высокий уровень (отлично) 5 баллов
УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий				
Результаты обучения: <i>Индикатор:</i> ИД-1 УК-1 выделяет проблемную ситуацию, осуществляет ее критический анализ и диагностику на основе системного подхода	с грубыми ошибками подбирает технологии поиска и критического анализа информации, использует методы системного подхода для решения поставленных задач с помощью цифровых и информационных технологий, организует личное цифровое пространство,	в основном подбирает технологии поиска и критического анализа информации, использует методы системного подхода для решения поставленных задач с помощью цифровых и информационных технологий, организует личное цифровое пространство,	подбирает технологии поиска и критического анализа информации, использует методы системного подхода для решения поставленных задач с помощью цифровых и информационных технологий, организует личное цифровое пространство,	в полном объеме подбирает технологии поиска и критического анализа информации, использует методы системного подхода для решения поставленных задач с помощью цифровых и информационных технологий, организует личное цифровое пространство,
ИД-2 УК-1 осуществляет поиск, сбор и обработку информации для определения альтернативных вариантов стратегических действий в проблемной ситуации	с грубыми ошибками определяет и оценивает риски возможных вариантов решений проблемной ситуации, выбирает оптимальный вариант её решения.	в основном осуществляет поиск, отбор и систематизацию информации для определения альтернативных вариантов стратегических решений в проблемной ситуации	осуществляет поиск, отбор и систематизацию информации для определения альтернативных вариантов стратегических решений в проблемной ситуации	в полном объеме осуществляет поиск, анализ, оценку, отбор и систематизацию информации для определения альтернативных вариантов стратегических решений в проблемной ситуации
ИД-3 УК-1 определяет и оценивает риски возможных вариантов решений проблемной ситуации, вырабатывает стратегию действий по решению проблемной ситуации	на низком уровне выделяет и оценивает риски возможных вариантов решений проблемной ситуации, вырабатывает стратегию действий по решению проблемной ситуации	в основном выделяет и оценивает риски возможных вариантов решений проблемной ситуации, вырабатывает стратегию действий по решению проблемной ситуации	выделяет и оценивает риски возможных вариантов решений проблемной ситуации, вырабатывает стратегию действий по решению проблемной ситуации	в полном объеме выделяет и оценивает риски возможных вариантов решений проблемной ситуации, вырабатывает стратегию действий по решению проблемной ситуации
УК -2 Способен управлять проектом на всех этапах его жизненного цикла				
ИД-1 УК-2 формулирует цель проекта, определяет совокупность взаимосвязанных задач,	на низком уровне осуществляет учёт требований законодательных и правовых актах РФ, регулирующих	в основном осуществляет учёт требований законодательных и правовых актах РФ, регулирующих	осуществляет учёт требований законодательных и правовых актах РФ, регулирующих правовые	в полном объеме осуществляет учёт требований законодательных и правовых актах РФ,

обеспечивающих ее достижение на всех этапах его жизненного цикла	правовые отношения в сфере информационной безопасности и защиты государственной тайны, применяет цифровые технологии для решения проектных задач, выбирая оптимальный способ их решения, исходя из действующих правовых норм и имеющихся ресурсов и ограничений	правовые отношения в сфере информационной безопасности и защиты государственной тайны, применяет цифровые технологии для решения проектных задач, выбирая оптимальный способ их решения, исходя из действующих правовых норм и имеющихся ресурсов и ограничений	отношения в сфере информационной безопасности и защиты государственной тайны, применяет цифровые технологии для решения проектных задач, выбирая оптимальный способ их решения, исходя из действующих правовых норм и имеющихся ресурсов и ограничений	регулирующих правовые отношения в сфере информационной безопасности и защиты государственной тайны, применяет цифровые технологии для решения проектных задач, выбирая оптимальный способ их решения, исходя из действующих правовых норм и имеющихся ресурсов и ограничений
ИД-2 УК-2 разрабатывает план действий по управлению проектом на всех этапах его жизненного цикла	с грубыми ошибками обеспечивает выполнение проекта в соответствии с установленными целями, сроками и затратами, исходя из действующих правовых норм, имеющихся ресурсов и ограничений, в том числе с использованием цифровых инструментов	в основном обеспечивает выполнение проекта в соответствии с установленными целями, сроками и затратами, исходя из действующих правовых норм, имеющихся ресурсов и ограничений, в том числе с использованием цифровых инструментов	обеспечивает выполнение проекта в соответствии с установленными целями, сроками и затратами, исходя из действующих правовых норм, имеющихся ресурсов и ограничений, в том числе с использованием цифровых инструментов	в полном объеме обеспечивает выполнение проекта в соответствии с установленными целями, сроками и затратами, исходя из действующих правовых норм, имеющихся ресурсов и ограничений, в том числе с использованием цифровых инструментов
ИД-3 УК-2 обеспечивает контроль выполнения и оценивает эффективность реализации проекта на всех этапах его жизненного цикла	с грубыми ошибками проводит контроль выполнения и оценивает эффективность реализации проекта на всех этапах его жизненного цикла	в основном проводит контроль выполнения и оценивает эффективность реализации проекта на всех этапах его жизненного цикла	проводит контроль выполнения и оценивает эффективность реализации проекта на всех этапах его жизненного цикла	в полном объеме проводит контроль выполнения и оценивает эффективность реализации проекта на всех этапах его жизненного цикла
УК -3 Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели				
ИД-1 УК-3 разрабатывает цель и задачи командной работы, используя инклюзивный подход,	ан низком уровне осознает свою роль в системе межличностного взаимодействия, анализирует	в основном осознает свою роль в системе межличностного взаимодействия, анализирует	осознает свою роль в системе межличностного взаимодействия, анализирует стратегии поведения в	в полном объеме осознает свою роль в системе межличностного взаимодействия, анализирует

эффективную коммуникацию, методы командообразования и командного взаимодействия при совместной работе	стратегии поведения в группе, и особенности поведения разных групп людей, с которыми работает (взаимодействует),	стратегии поведения в группе, и особенности поведения разных групп людей, с которыми работает (взаимодействует),	группе, и особенности поведения разных групп людей, с которыми работает (взаимодействует),	стратегии поведения в группе, и особенности поведения разных групп людей, с которыми работает (взаимодействует),
ИД-2 УК-3 организует работу команды для получения оптимальных результатов совместной работы, с учетом индивидуальных возможностей её членов, использования методологии достижения успеха, методов, информационных технологий и технологий фортсайта	с грубыми ошибками определяет статус и роль членов группы в системе межличностных отношений и учитывает на практике эти показатели, применяет методы командной работы, обеспечивает выполнение поставленных задач на основе мониторинга командной работы и своевременного реагирования на существенные отклонения.	в основном определяет статус и роль членов группы в системе межличностных отношений и учитывает на практике эти показатели, применяет методы командной работы, обеспечивает выполнение поставленных задач на основе мониторинга командной работы и своевременного реагирования на существенные отклонения.	определяет статус и роль членов группы в системе межличностных отношений и учитывает на практике эти показатели, применяет методы командной работы, обеспечивает выполнение поставленных задач на основе мониторинга командной работы и своевременного реагирования на существенные отклонения.	в полном объеме определяет статус и роль членов группы в системе межличностных отношений и учитывает на практике эти показатели, применяет методы командной работы, обеспечивает выполнение поставленных задач на основе мониторинга командной работы и своевременного реагирования на существенные отклонения.
ИД-3 УК-3 руководит выполнением поставленных задач на основе мониторинга командной работы и своевременного реагирования на существенные отклонения	с грубыми ошибками руководит выполнением поставленных задач на основе мониторинга командной работы и своевременного реагирования на существенные отклонения	в основном руководит выполнением поставленных задач на основе мониторинга командной работы и своевременного реагирования на существенные отклонения	руководит выполнением поставленных задач на основе мониторинга командной работы и своевременного реагирования на существенные отклонения	в полном объеме руководит выполнением поставленных задач на основе мониторинга командной работы и своевременного реагирования на существенные отклонения
УК-4 Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия				
ИД-1 УК-4 выбирает приемлемый стиль делового общения на государственном(-ых) и иностранном(-ых) языках, вербальные и невербальные	на низком уровне руководствуется правилами деловой коммуникации в устной и письменной формах на государственном языке РФ и иностранном(ых) языке(ах),	в основном руководствуется правилами деловой коммуникации в устной и письменной формах на государственном языке РФ и иностранном(ых) языке(ах),	руководствуется правилами деловой коммуникации в устной и письменной формах на государственном языке РФ и иностранном(ых) языке(ах), пользуется	в полном руководствуется правилами деловой коммуникации в устной и письменной формах на государственном языке РФ и иностранном(ых) языке(ах),

средства взаимодействия с партнерами в устной и письменной формах	пользуется современными средствами деловой коммуникации на основе информационных технологий, осуществляет поиск и анализ требуемой информации в профессиональном взаимодействии, проводит оценку эффективности применяемых информационных технологий	пользуется современными средствами деловой коммуникации на основе информационных технологий, осуществляет поиск и анализ требуемой информации в профессиональном взаимодействии, проводит оценку эффективности применяемых информационных технологий	современными средствами деловой коммуникации на основе информационных технологий, осуществляет поиск и анализ требуемой информации в профессиональном взаимодействии, проводит оценку эффективности применяемых информационных технологий	пользуется современными средствами деловой коммуникации на основе информационных технологий, осуществляет поиск и анализ требуемой информации в профессиональном взаимодействии, проводит оценку эффективности применяемых информационных технологий
ИД-2 УК-4 применяет современные коммуникационные технологии для повышения эффективности профессионального взаимодействия, поиска необходимой информации в процессе решения стандартных коммуникативных задач на государственном(-ых) и иностранном(-ых) языках	допускает грубые ошибки при решении профессиональных задач с использованием современных коммуникационных технологий, при поиске необходимой информации в процессе решения стандартных коммуникативных задач на государственном(-ых) и иностранном(-ых) языках	в основном решает профессиональные задачи с использованием современных коммуникационных технологий, проводит поиск необходимой информации в процессе решения стандартных коммуникативных задач на государственном(-ых) и иностранном(-ых) языках	решает профессиональные задачи с использованием современных коммуникационных технологий, проводит поиск необходимой информации в процессе решения стандартных коммуникативных задач на государственном(-ых) и иностранном(-ых) языках	в полном объеме решает профессиональные задачи с использованием современных коммуникационных технологий, проводит поиск необходимой информации в процессе решения стандартных коммуникативных задач на государственном(-ых) и иностранном(-ых) языках
ИД-3 УК-4 оценивает эффективность применяемых коммуникативных технологий в профессиональном взаимодействии на государственном (-ых) и иностранном (-ых) языках,	на низком уровне проводит оценку эффективности применяемых коммуникативных технологий в профессиональном взаимодействии на государственном (-ых) и иностранном (-ых) языках, производит выбор	в основном проводит оценку эффективности применяемых коммуникативных технологий в профессиональном взаимодействии на государственном (-ых) и иностранном (-ых) языках,	проводит оценку эффективности применяемых коммуникативных технологий в профессиональном взаимодействии на государственном (-ых) и иностранном (-ых) языках,	в полном объеме проводит оценку эффективности применяемых коммуникативных технологий в профессиональном взаимодействии на государственном (-ых) и иностранном (-ых) языках,

производит оптимальных	выбор оптимальных решений	производит оптимальных решений	производит оптимальных решений	производит оптимальных решений
УК-5 Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия				
ИД-1 УК-5 - выявляет, сопоставляет и анализирует информацию о культурных особенностях и традициях различных социальных групп, для выбора стратегии взаимодействия с их носителями	на низком уровне учитывает культурные особенности и традиции различных социальных групп, этносов и конфессий, анализируя социальные ситуации взаимодействия	в основном учитывает культурные особенности и традиции различных социальных групп, этносов и конфессий, анализируя социальные ситуации взаимодействия	учитывает культурные особенности и традиции различных социальных групп, этносов и конфессий, анализируя социальные ситуации взаимодействия	в полном объеме учитывает культурные особенности и традиции различных социальных групп, этносов и конфессий, анализируя социальные ситуации взаимодействия
ИД-2 УК-5 демонстрирует уважительное отношение к историческому наследию и социокультурным традициям различных социальных групп, опирающееся на знание этапов исторического развития России (включая основные события, основных исторических деятелей) в контексте мировой истории и ряда культурных традиций мира (в зависимости от среды и задач образования), включая мировые религии, философские и этические учения	на низком уровне проявляет уважение к историческому наследию и социокультурным традициям различных социальных групп, опирающееся на знание этапов исторического развития России (включая основные события, основных исторических деятелей) в контексте мировой истории и ряда культурных традиций мира (в зависимости от среды и задач образования), включая мировые религии, философские и этические учения	в основном проявляет уважение к историческому наследию и социокультурным традициям различных социальных групп, опирающееся на знание этапов исторического развития России (включая основные события, основных исторических деятелей) в контексте мировой истории и ряда культурных традиций мира (в зависимости от среды и задач образования), включая мировые религии, философские и этические учения	проявляет уважение к историческому наследию и социокультурным традициям различных социальных групп, опирающееся на знание этапов исторического развития России (включая основные события, основных исторических деятелей) в контексте мировой истории и ряда культурных традиций мира (в зависимости от среды и задач образования), включая мировые религии, философские и этические учения	в полном объеме проявляет уважение к историческому наследию и социокультурным традициям различных социальных групп, опирающееся на знание этапов исторического развития России (включая основные события, основных исторических деятелей) в контексте мировой истории и ряда культурных традиций мира (в зависимости от среды и задач образования), включая мировые религии, философские и этические учения
ИД-3 УК-5 - выбирает способы конструктивного взаимодействия с людьми с учетом их социокультурных	на низком уровне выбирает формы, методы, приемы взаимодействия с различными социальными группами,	в основном выбирает формы, методы, приемы взаимодействия с различными социальными	выбирает формы, методы, приемы взаимодействия с различными социальными группами, учитывает	в полном объеме выбирает формы, методы, приемы взаимодействия с различными социальными

особенностей в целях успешного выполнения профессиональных задач и усиления социальной интеграции	учитывает культурные и религиозные традиции, при личном и массовом общении, определяет приемы конструктивного взаимодействия в ситуации общения	группами, учитывает культурные и религиозные традиции, при личном и массовом общении, определяет приемы конструктивного взаимодействия в ситуации общения	культурные и религиозные традиции, при личном и массовом общении, определяет приемы конструктивного взаимодействия в ситуации общения	группами, учитывает культурные и религиозные традиции, при личном и массовом общении, определяет приемы конструктивного взаимодействия в ситуации общения
УК – 6 Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни				
ИД-1 УК-6 устанавливает личные и профессиональные цели в соответствии с уровнем своих ресурсов и приоритетов действий, для успешного развития в избранной сфере профессиональной деятельности	допускает грубые ошибки, при постановке целей в своей профессиональной деятельности и решении профессиональных задач с учётом своих ресурсных возможностей и приоритетов, выбирает эффективные стратегии и тактики личностного и профессионального развития, пользуется методикой оценки применяемых методов решения поставленных задач в сфере своей профессиональной деятельности	в основном ставит цели в своей профессиональной деятельности и решает профессиональные задачи с учётом своих ресурсных возможностей и приоритетов, выбирает эффективные стратегии и тактики личностного и профессионального развития, пользуется методикой оценки применяемых методов решения поставленных задач в сфере своей профессиональной деятельности	ставит цели в своей профессиональной деятельности и решает профессиональные задачи с учётом своих ресурсных возможностей и приоритетов, выбирает эффективные стратегии и тактики личностного и профессионального развития, пользуется методикой оценки применяемых методов решения поставленных задач в сфере своей профессиональной деятельности	в полном объёме ставит цели в своей профессиональной деятельности и решает профессиональные задачи с учётом своих ресурсных возможностей и приоритетов, выбирает эффективные стратегии и тактики личностного и профессионального развития, пользуется методикой оценки применяемых методов решения поставленных задач в сфере своей профессиональной деятельности
ИД-2 УК-6 реализует и корректирует стратегию своего личностного и профессионального развития с учетом условий, средств, личностных	с грубыми ошибками оценивает эффективность использования времени и других ресурсов при решении поставленных задач в избранной сфере	в основном оценивает эффективность использования времени и других ресурсов при решении поставленных задач в избранной сфере	оценивает эффективность использования времени и других ресурсов при решении поставленных задач в избранной сфере профессиональной	в полном объёме оценивает эффективность использования времени и других ресурсов при решении поставленных задач в избранной сфере

возможностей, этапов карьерного роста, временной перспективы развития деятельности и требований рынка труда	профессиональной деятельности	профессиональной деятельности	деятельности	профессиональной деятельности
ИД-3 УК-6 критически оценивает эффективность использования своего времени и других ресурсов при решении задач, поставленных в избранной сфере профессиональной деятельности	с грубыми ошибками проводит критическую оценку эффективности использования своего времени и других ресурсов, при решении задач, поставленных в избранной сфере профессиональной деятельности	в основном проводит критическую оценку эффективности использования своего времени и других ресурсов, при решении задач, поставленных в избранной сфере профессиональной деятельности	проводит критическую оценку эффективности использования своего времени и других ресурсов, при решении задач, поставленных в избранной сфере профессиональной деятельности	в полном объеме проводит критическую оценку эффективности использования своего времени и других ресурсов, при решении задач, поставленных в избранной сфере профессиональной деятельности
ОПК – 1 Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание				
ИД-1 ОПК-1 проектирует информационные системы с учетом различных технологий обеспечения информационной безопасности	допускает грубые ошибки при решении задач моделирования и проектирования автоматизированных информационных систем и систем обеспечения информационной безопасности, разработке и обосновании критериев оценки эффективности проектируемой системы обеспечения информационной безопасности	в основном применяет методы решения задач моделирования и проектирования автоматизированных информационных систем и систем обеспечения информационной безопасности, разрабатывает и обосновывает критерии оценки эффективности проектируемой системы обеспечения информационной безопасности	применяет методы решения задач моделирования и проектирования автоматизированных информационных систем и систем обеспечения информационной безопасности, разрабатывает и обосновывает критерии оценки эффективности проектируемой системы обеспечения информационной безопасности	в полном объеме применяет методы решения задач моделирования и проектирования автоматизированных информационных систем и систем обеспечения информационной безопасности, разрабатывает и обосновывает критерии оценки эффективности проектируемой системы обеспечения информационной безопасности
ИД-2 ОПК-1 формирует актуальную модель угроз для автоматизированных	с грубыми ошибками разрабатывает актуальную модель угроз для	в основном разрабатывает актуальную модель угроз для автоматизированных	разрабатывает актуальную модель угроз для автоматизированных	в полном объеме разрабатывает актуальную модель угроз для

информационных систем и учитывает её положения при формировании требований технического задания на проектируемую систему обеспечения информационной безопасности	автоматизированных информационных систем и учитывает её положения при формировании требований технического задания на проектируемую систему обеспечения информационной безопасности	информационных систем и учитывает её положения при формировании требований технического задания на проектируемую систему обеспечения информационной безопасности	информационных систем и учитывает её положения при формировании требований технического задания на проектируемую систему обеспечения информационной безопасности	автоматизированных информационных систем и учитывает её положения при формировании требований технического задания на проектируемую систему обеспечения информационной безопасности
ИД-3 ОПК-1 разрабатывает и обосновывает критерии оценки эффективности проектируемой системы обеспечения информационной безопасности, оценивает эффективность решений и анализирует показатели деятельности	с грубыми ошибками проводит разработку и обосновывает критерии оценки эффективности проектируемой системы обеспечения информационной безопасности, оценивает эффективность решений и анализирует показатели деятельности	в основном проводит разработку и обосновывает критерии оценки эффективности проектируемой системы обеспечения информационной безопасности, оценивает эффективность решений и анализирует показатели деятельности	проводит разработку и обосновывает критерии оценки эффективности проектируемой системы обеспечения информационной безопасности, оценивает эффективность решений и анализирует показатели деятельности	в полном объёме проводит разработку и обосновывает критерии оценки эффективности проектируемой системы обеспечения информационной безопасности, оценивает эффективность решений и анализирует показатели деятельности
ОПК – 2 Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности				
ИД-1 ОПК-2 использует методы концептуального проектирования технологий обеспечения информационной безопасности	допускает грубые ошибки при определении направления развития и проблем компьютерного моделирования сложных систем, разработке и исследовании системы защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасности	в основном определяет направления развития и проблем компьютерного моделирования сложных систем, разработке и исследовании системы защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасности	определяет направления развития и проблем компьютерного моделирования сложных систем, разработке и исследовании системы защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасности	в полном объёме определяет направления развития и проблем компьютерного моделирования сложных систем, разработке и исследовании системы защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасности
ИД-2 ОПК-2 выбирает и обосновывает преимущества	на низком уровне реализовывает типовые задачи	в основном реализовывает типовые задачи средствами	реализовывает типовые задачи средствами	в полном объёме реализовывает типовые задачи

методов решения задач для защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью	средствами автоматизированного и ручного функционального тестирования	автоматизированного и ручного функционального тестирования	автоматизированного и ручного функционального тестирования	задачи средствами автоматизированного и ручного функционального тестирования
ИД-3 ОПК-2 решает типовые задачи разработки и исследования систем защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью	на низком уровне учитывает направления развития технологий проектирования информационных, автоматизированных и автоматических систем, управляет коллективом исполнителей и принимает управленческие решения,	в основном учитывает направления развития технологий проектирования информационных, автоматизированных и автоматических систем, управляет коллективом исполнителей и принимает управленческие решения,	учитывает направления развития технологий проектирования информационных, автоматизированных и автоматических систем, управляет коллективом исполнителей и принимает управленческие решения,	в полном объеме учитывает направления развития технологий проектирования информационных, автоматизированных и автоматических систем, управляет коллективом исполнителей и принимает управленческие решения,
ОПК – 3 Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности				
ИД-1 ОПК-3 разрабатывает технические задания на создание подсистем обеспечения информационной безопасности	допускает грубые ошибки при соблюдении правил построения оптимальной политики безопасности в соответствии с требованиями уровня безопасности, определении стоимости и сроков реализации проекта, выполнении работ с нормативными правовыми актами в области информационной безопасности с технической и эксплуатационной документацией, при оценке различных инструментов в области проектирования и управления информационной	в основном соблюдает правила построения оптимальной политики безопасности в соответствии с требованиями уровня безопасности, определяет стоимость и сроки реализации проекта, работает с нормативными правовыми актами в области информационной безопасности с технической и эксплуатационной документацией, оценивает различные инструменты в области проектирования и управления информационной	соблюдает правила построения оптимальной политики безопасности в соответствии с требованиями уровня безопасности, определяет стоимость и сроки реализации проекта, работает с нормативными правовыми актами в области информационной безопасности с технической и эксплуатационной документацией, оценивает различные инструменты в области проектирования и управления информационной	в полном объеме соблюдает правила построения оптимальной политики безопасности в соответствии с требованиями уровня безопасности, определяет стоимость и сроки реализации проекта, работает с нормативными правовыми актами в области информационной безопасности с технической и эксплуатационной документацией, оценивает различные инструменты в области проектирования и управления информационной

	безопасности	безопасности	безопасности	безопасности
ИД-2 ОПК-3 разрабатывает проекты организационно-распорядительной документации по обеспечению информационной безопасности	допускает грубые ошибки при учёте требований отечественных и зарубежных стандартов в области сертификации и аттестации объектов информатизации, определении основных угроз безопасности информации и моделей нарушителя в информационных системах, разработке политик безопасности различных уровней, расчёте и разработке положения о применимости механизмов контроля в контексте управления рисками информационной безопасности	в основном соблюдает основы отечественных и зарубежных стандартов в области сертификации и аттестации объектов информатизации, учитывает основные угрозы безопасности информации и модели нарушителя в информационных системах, разрабатывает политики безопасности различных уровней, рассчитывает и разрабатывает положения о применимости механизмов контроля в контексте управления рисками информационной безопасности	соблюдает основы отечественных и зарубежных стандартов в области сертификации и аттестации объектов информатизации, учитывает основные угрозы безопасности информации и модели нарушителя в информационных системах, разрабатывает политики безопасности различных уровней, рассчитывает и разрабатывает положения о применимости механизмов контроля в контексте управления рисками информационной безопасности	в полном объёме соблюдает основы отечественных и зарубежных стандартов в области сертификации и аттестации объектов информатизации, учитывает основные угрозы безопасности информации и модели нарушителя в информационных системах, разрабатывает политики безопасности различных уровней, рассчитывает и разрабатывает положения о применимости механизмов контроля в контексте управления рисками информационной безопасности
ИД-3 ОПК-3 проводит технико-экономическое обоснование проектных решений в области построения систем обеспечения информационной безопасности	допускает грубые ошибки при соблюдении правил построения оптимальной политики безопасности в соответствии с требованиями уровня безопасности, определении стоимости и сроков реализации проекта, выполнении работ с нормативными правовыми актами в области информационной безопасности с технической и эксплуатационной	в основном соблюдает правила построения оптимальной политики безопасности в соответствии с требованиями уровня безопасности, определяет стоимость и сроки реализации проекта, работает с нормативными правовыми актами в области информационной безопасности с технической и эксплуатационной документацией, оценивает	соблюдает правила построения оптимальной политики безопасности в соответствии с требованиями уровня безопасности, определяет стоимость и сроки реализации проекта, работает с нормативными правовыми актами в области информационной безопасности с технической и эксплуатационной документацией, оценивает	в полном объёме соблюдает правила построения оптимальной политики безопасности в соответствии с требованиями уровня безопасности, определяет стоимость и сроки реализации проекта, работает с нормативными правовыми актами в области информационной безопасности с технической и эксплуатационной документацией, оценивает

	документацией, при оценке различных инструментов в области проектирования и управления информационной безопасности	различные инструменты в области проектирования и управления информационной безопасности	различные инструменты в области проектирования и управления информационной безопасности	различные инструменты в области проектирования и управления информационной безопасности
ОПК-4 Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок				
ИД-1 ОПК-4 осуществляет сбор и обработку информации в глобальной компьютерной сети, проводит анализ научно-технической информации по теме исследования	с грубыми ошибками формулирует научную проблему, анализирует гипотезы, проводит выбор предмета, объекта, целей, задач исследования, создаёт эскизный, технический, рабочий проект, применяет технологии поиска, изучения, обобщения и систематизации научной информации,	в основном формулирует научную проблему, анализирует гипотезы, проводит выбор предмета, объекта, целей, задач исследования, создаёт эскизный, технический, рабочий проект, применяет технологии поиска, изучения, обобщения и систематизации научной информации	формулирует научную проблему, анализирует гипотезы, проводит выбор предмета, объекта, целей, задач исследования, создаёт эскизный, технический, рабочий проект, применяет технологии поиска, изучения, обобщения и систематизации научной информации	в полном объёме формулирует научную проблему, анализирует гипотезы, проводит выбор предмета, объекта, целей, задач исследования, создаёт эскизный, технический, рабочий проект, применяет технологии поиска, изучения, обобщения и систематизации научной информации
ИД-2 ОПК-4 разрабатывает пошаговый план и программу научной деятельности, проводит предпроектные исследования	с грубыми ошибками определяет комплекс мер для обеспечения безопасности информационных систем, составляет аналитические обзоры по вопросам обеспечения информационной безопасности систем, использует методы и средства анализа защищенности информационных систем, программные и аппаратные средства персонального компьютера для поиска и обработки информации	в основном определяет комплекс мер для обеспечения безопасности информационных систем, составляет аналитические обзоры по вопросам обеспечения информационной безопасности систем, использует методы и средства анализа защищенности информационных систем, программные и аппаратные средства персонального	определяет комплекс мер для обеспечения безопасности информационных систем, составляет аналитические обзоры по вопросам обеспечения информационной безопасности систем, использует методы и средства анализа защищенности информационных систем, программные и аппаратные средства персонального	в полном объёме определяет комплекс мер для обеспечения безопасности информационных систем, составляет аналитические обзоры по вопросам обеспечения информационной безопасности систем, использует методы и средства анализа защищенности информационных систем, программные и аппаратные средства персонального

		компьютера для поиска и обработки информации	компьютера для поиска и обработки информации	компьютера для поиска и обработки информации
ИД-3 ОПК-4 применяет методику создания технического задания и технического проекта при организации НИОКР	с грубыми ошибками формулирует научную проблему, анализирует гипотезы, применяет методику создания технического задания и технического проекта при организации НИОКР	в основном формулирует научную проблему, анализирует гипотезы, применяет методику создания технического задания и технического проекта при организации НИОКР	формулирует научную проблему, анализирует гипотезы, применяет методику создания технического задания и технического проекта при организации НИОКР	в полном объеме формулирует научную проблему, анализирует гипотезы, применяет методику создания технического задания и технического проекта при организации НИОКР
ОПК-5 Способен проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи.				
ИД-1 ОПК-5 применяет методы научных исследований в научной деятельности, в частности, при написании магистерской диссертации и научных статей	с грубыми ошибками определяет порядок организации процесса исследования, методы построения оптимальных планов для научных экспериментов, оформляет научные публикации в соответствии с шаблоном IEEE, требованиями научных конференций	в основном определяет порядок организации процесса исследования, методы построения оптимальных планов для научных экспериментов, оформляет научные публикации в соответствии с шаблоном IEEE, требованиями научных конференций	определяет порядок организации процесса исследования, методы построения оптимальных планов для научных экспериментов, оформляет научные публикации в соответствии с шаблоном IEEE, требованиями научных конференций	в полном объеме определяет порядок организации процесса исследования, методы построения оптимальных планов для научных экспериментов, оформляет научные публикации в соответствии с шаблоном IEEE, требованиями научных конференций
ИД-2 ОПК-5 оформляет научно-технические отчеты и обзоры по результатам проведенных экспериментальных исследований	с грубыми ошибками разрабатывает техническую документацию в соответствии с требованиями Единой системы конструкторской документации и Единой системы программной документации, анализирует получаемые результаты и формулирует выводы	в основном разрабатывает техническую документацию в соответствии с требованиями Единой системы конструкторской документации и Единой системы программной документации, анализирует получаемые результаты и формулирует выводы	разрабатывает техническую документацию в соответствии с требованиями Единой системы конструкторской документации и Единой системы программной документации, анализирует получаемые результаты и формулирует выводы	в полном объеме разрабатывает техническую документацию в соответствии с требованиями Единой системы конструкторской документации и Единой системы программной документации, анализирует получаемые результаты и формулирует выводы

ИД-3 ОПК-5 готовит научные доклады и статьи по результатам выполненных исследований	с грубыми ошибками выбирает и обосновывает критерии оценки защищенности открытых информационных систем, готовит научные доклады и статьи	в основном выбирает и обосновывает критерии оценки защищенности открытых информационных систем, готовит научные доклады и статьи	выбирает и обосновывает критерии оценки защищенности открытых информационных систем, готовит научные доклады и статьи	в полном объеме выбирает и обосновывает критерии оценки защищенности открытых информационных систем, готовит научные доклады и статьи
---	--	--	---	---

8.2 Критерии оценивания компетенций на государственном экзамене

Оценка «отлично» выставляется обучающему, если студент на высоком уровне подбирает технологии поиска и критического анализа информации, использует методы системного подхода для решения поставленных задач с помощью цифровых и информационных технологий, организует личное цифровое пространство, осуществляет поиск, отбор и систематизацию информации для определения альтернативных вариантов стратегических решений в проблемной ситуации, выделяет и оценивает риски возможных вариантов решений проблемной ситуации, вырабатывает стратегию действий по решению проблемной ситуации, осуществляет учёт требований законодательных и правовых актов РФ, регулирующих правовые отношения в сфере информационной безопасности и защиты государственной тайны, применяет цифровые технологии для решения проектных задач, выбирая оптимальный способ их решения, исходя из действующих правовых норм и имеющихся ресурсов и ограничений, обеспечивает выполнение проекта в соответствии с установленными целями, сроками и затратами, исходя из действующих правовых норм, имеющихся ресурсов и ограничений, в том числе с использованием цифровых инструментов, проводит контроль выполнения и оценивает эффективность реализации проекта на всех этапах его жизненного цикла, осознает свою роль в системе межличностного взаимодействия, анализирует стратегии поведения в группе, и особенности поведения разных групп людей, с которыми работает (взаимодействует), определяет статус и роль членов группы в системе межличностных отношений и учитывает на практике эти показатели, применяет методы командной работы, обеспечивает выполнение поставленных задач на основе мониторинга командной работы и своевременного реагирования на существенные отклонения, руководит выполнением поставленных задач на основе мониторинга командной работы и своевременного реагирования на существенные отклонения, руководствуется правилами деловой коммуникации в устной и письменной формах на государственном языке РФ и иностранном(ых) языке(ах), пользуется современными средствами деловой коммуникации на основе информационных технологий, осуществляет поиск и анализ требуемой информации в профессиональном взаимодействии, проводит оценку эффективности применяемых информационных технологий, решает профессиональные задачи с использованием современных коммуникационных технологий, проводит поиск необходимой информации в процессе решения стандартных коммуникативных задач на государственном(-ых) и иностранном(-ых) языках, проводит оценку эффективности применяемых коммуникативных технологий в профессиональном взаимодействии на государственном (-ых) и иностранном (-ых) языках, производит выбор оптимальных решений, учитывает культурные особенности и традиции различных социальных групп, этносов и конфессий, анализируя социальные ситуации взаимодействия, проявляет уважение к историческому наследию и социокультурным традициям различных социальных групп, опирающееся на знание этапов исторического развития России (включая основные события, основных исторических деятелей) в контексте мировой истории и ряда культурных традиций мира (в зависимости от среды и задач образования), включая мировые религии, философские и этические учения, выбирает формы, методы, приемы взаимодействия с различными социальными группами, учитывает культурные и религиозные традиции, при личном и массовом общении, определяет приемы конструктивного взаимодействия в ситуации общения, ставит цели в своей профессиональной деятельности и решает профессиональные задачи с учётом своих ресурсных возможностей и приоритетов, выбирает эффективные стратегии и тактики личностного и профессионального развития, пользуется методикой оценки эффективности применяемых методов решения поставленных задач в сфере своей профессиональной деятельности, оценивает эффективность использования времени и других ресурсов при решении поставленных задач в избранной сфере профессиональной деятельности, проводит критическую оценку эффективности использования своего времени и других ресурсов, при решении задач, поставленных в избранной сфере профессиональной деятельности, применяет

методы решения задач моделирования и проектирования автоматизированных информационных систем и систем обеспечения информационной безопасности, разрабатывает и обосновывает критерии оценки эффективности проектируемой системы обеспечения информационной безопасности, разрабатывает актуальную модель угроз для автоматизированных информационных систем и учитывает её положения при формировании требований технического задания на проектируемую систему обеспечения информационной безопасности, проводит разработку и обосновывает критерии оценки эффективности проектируемой системы обеспечения информационной безопасности, оценивает эффективность решений и анализирует показатели деятельности, определяет направления развития и проблем компьютерного моделирования сложных систем, разработке и исследовании системы защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасности, реализовывает типовые задачи средствами автоматизированного и ручного функционального тестирования, учитывает направления развития технологий проектирования информационных, автоматизированных и автоматических систем, управляет коллективом исполнителей и принимает управленческие решения, соблюдает правила построения оптимальной политики безопасности в соответствии с требованиями уровня безопасности, определяет стоимость и сроки реализации проекта, работает с нормативными правовыми актами в области информационной безопасности с технической и эксплуатационной документацией, оценивает различные инструменты в области проектирования и управления информационной безопасности, соблюдает основы отечественных и зарубежных стандартов в области сертификации и аттестации объектов информатизации, учитывает основные угрозы безопасности информации и модели нарушителя в информационных системах, разрабатывает политики безопасности различных уровней, рассчитывает и разрабатывает положения о применимости механизмов контроля в контексте управления рисками информационной безопасности, соблюдает правила построения оптимальной политики безопасности в соответствии с требованиями уровня безопасности, определяет стоимость и сроки реализации проекта, работает с нормативными правовыми актами в области информационной безопасности с технической и эксплуатационной документацией, оценивает различные инструменты в области проектирования и управления информационной безопасности, соблюдает основы отечественных и зарубежных стандартов в области сертификации и аттестации объектов информатизации, учитывает основные угрозы безопасности информации и модели нарушителя в информационных системах, разрабатывает политики безопасности различных уровней, рассчитывает и разрабатывает положения о применимости механизмов контроля в контексте управления рисками информационной безопасности, формулирует научную проблему, анализирует гипотезы, проводит выбор предмета, объекта, целей, задач исследования, создаёт эскизный, технический, рабочий проект, применяет технологии поиска, изучения, обобщения и систематизации научной информации, определяет комплекс мер для обеспечения безопасности информационных систем, составляет аналитические обзоры по вопросам обеспечения информационной безопасности систем, использует методы и средства анализа защищенности информационных систем, программные и аппаратные средства персонального компьютера для поиска и обработки информации, формулирует научную проблему, анализирует гипотезы, применяет методику создания технического задания и технического проекта при организации НИОКР, определяет порядок организации процесса исследования, методы построения оптимальных планов для научных экспериментов, оформляет научные публикации в соответствии с шаблоном IEEE, требованиями научных конференций, разрабатывает техническую документацию в соответствии с требованиями Единой системы конструкторской документации и Единой системы программной документации, анализирует получаемые результаты и формулирует выводы, выбирает и обосновывает критерии оценки защищенности открытых информационных систем, готовит научные доклады и статьи.

Оценка «хорошо» выставляется обучающему, если студент на хорошем уровне подбирает технологии поиска и критического анализа информации, использует методы системного подхода для решения поставленных задач с помощью цифровых и информационных технологий, организует личное цифровое пространство, осуществляет поиск, отбор и систематизацию информации для определения альтернативных вариантов стратегических решений в проблемной ситуации, выделяет и оценивает риски возможных вариантов решений проблемной ситуации, вырабатывает стратегию действий по решению проблемной ситуации, осуществляет учёт требований законодательных и правовых актов РФ, регулирующих правовые отношения в сфере информационной безопасности и защиты государственной тайны, применяет цифровые технологии для решения проектных задач, выбирая оптимальный способ их решения, исходя из действующих правовых норм и имеющихся ресурсов и ограничений, обеспечивает выполнение проекта в соответствии с установленными целями, сроками и затратами, исходя из действующих правовых норм, имеющихся ресурсов и ограничений, в том числе с использованием цифровых инструментов, проводит контроль выполнения и оценивает эффективность реализации проекта на всех этапах его жизненного цикла, осознает свою роль в системе межличностного взаимодействия, анализирует стратегии поведения в группе, и особенности поведения разных групп людей, с которыми работает (взаимодействует), определяет статус и роль членов группы в системе межличностных отношений и учитывает на практике эти показатели, применяет методы командной работы, обеспечивает выполнение поставленных задач на основе мониторинга командной работы и своевременного реагирования на существенные отклонения, руководит выполнением поставленных задач на основе мониторинга командной работы и своевременного реагирования на существенные отклонения, руководствуется правилами деловой коммуникации в устной и письменной формах на государственном языке РФ и иностранном(ых) языке(ах), пользуется современными средствами деловой коммуникации на основе информационных технологий, осуществляет поиск и анализ требуемой информации в профессиональном взаимодействии, проводит оценку эффективности применяемых информационных технологий, решает профессиональные задачи с использованием современных коммуникационных технологий, проводит поиск необходимой информации в процессе решения стандартных коммуникативных задач на государственном(-ых) и иностранном(-ых) языках, проводит оценку эффективности применяемых коммуникативных технологий в профессиональном взаимодействии на государственном (-ых) и иностранном (-ых) языках, производит выбор оптимальных решений, учитывает культурные особенности и традиции различных социальных групп, этносов и конфессий, анализируя социальные ситуации взаимодействия, проявляет уважение к историческому наследию и социокультурным традициям различных социальных групп, опирающееся на знание этапов исторического развития России (включая основные события, основных исторических деятелей) в контексте мировой истории и ряда культурных традиций мира (в зависимости от среды и задач образования), включая мировые религии, философские и этические учения, выбирает формы, методы, приемы взаимодействия с различными социальными группами, учитывает культурные и религиозные традиции, при личном и массовом общении, определяет приемы конструктивного взаимодействия в ситуации общения, ставит цели в своей профессиональной деятельности и решает профессиональные задачи с учётом своих ресурсных возможностей и приоритетов, выбирает эффективные стратегии и тактики личностного и профессионального развития, пользуется методикой оценки эффективности применяемых методов решения поставленных задач в сфере своей профессиональной деятельности, оценивает эффективность использования времени и других ресурсов при решении поставленных задач в избранной сфере профессиональной деятельности, проводит критическую оценку эффективности использования своего времени и других ресурсов, при решении задач, поставленных в избранной сфере профессиональной деятельности, применяет методы решения задач моделирования и проектирования автоматизированных информационных систем и систем обеспечения информационной безопасности,

разрабатывает и обосновывает критерии оценки эффективности проектируемой системы обеспечения информационной безопасности, разрабатывает актуальную модель угроз для автоматизированных информационных систем и учитывает её положения при формировании требований технического задания на проектируемую систему обеспечения информационной безопасности, проводит разработку и обосновывает критерии оценки эффективности проектируемой системы обеспечения информационной безопасности, оценивает эффективность решений и анализирует показатели деятельности, определяет направления развития и проблем компьютерного моделирования сложных систем, разработке и исследовании системы защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасности, реализовывает типовые задачи средствами автоматизированного и ручного функционального тестирования, учитывает направления развития технологий проектирования информационных, автоматизированных и автоматических систем, управляет коллективом исполнителей и принимает управленческие решения, соблюдает правила построения оптимальной политики безопасности в соответствии с требованиями уровня безопасности, определяет стоимость и сроки реализации проекта, работает с нормативными правовыми актами в области информационной безопасности с технической и эксплуатационной документацией, оценивает различные инструменты в области проектирования и управления информационной безопасностью, соблюдает основы отечественных и зарубежных стандартов в области сертификации и аттестации объектов информатизации, учитывает основные угрозы безопасности информации и модели нарушителя в информационных системах, разрабатывает политики безопасности различных уровней, рассчитывает и разрабатывает положения о применимости механизмов контроля в контексте управления рисками информационной безопасности, соблюдает правила построения оптимальной политики безопасности в соответствии с требованиями уровня безопасности, определяет стоимость и сроки реализации проекта, работает с нормативными правовыми актами в области информационной безопасности с технической и эксплуатационной документацией, оценивает различные инструменты в области проектирования и управления информационной безопасностью, соблюдает основы отечественных и зарубежных стандартов в области сертификации и аттестации объектов информатизации, учитывает основные угрозы безопасности информации и модели нарушителя в информационных системах, разрабатывает политики безопасности различных уровней, рассчитывает и разрабатывает положения о применимости механизмов контроля в контексте управления рисками информационной безопасности, формулирует научную проблему, анализирует гипотезы, проводит выбор предмета, объекта, целей, задач исследования, создаёт эскизный, технический, рабочий проект, применяет технологии поиска, изучения, обобщения и систематизации научной информации, определяет комплекс мер для обеспечения безопасности информационных систем, составляет аналитические обзоры по вопросам обеспечения информационной безопасности систем, использует методы и средства анализа защищенности информационных систем, программные и аппаратные средства персонального компьютера для поиска и обработки информации, формулирует научную проблему, анализирует гипотезы, применяет методику создания технического задания и технического проекта при организации НИОКР, определяет порядок организации процесса исследования, методы построения оптимальных планов для научных экспериментов, оформляет научные публикации в соответствии с шаблоном IEEE, требованиями научных конференций, разрабатывает техническую документацию в соответствии с требованиями Единой системы конструкторской документации и Единой системы программной документации, анализирует получаемые результаты и формулирует выводы, выбирает и обосновывает критерии оценки защищенности открытых информационных систем, готовит научные доклады и статьи.

Оценка «удовлетворительно» выставляется обучающему, если студент на удовлетворительном уровне подбирает технологии поиска и критического анализа информации, использует методы системного подхода для решения поставленных задач с

помощью цифровых и информационных технологий, организует личное цифровое пространство, осуществляет поиск, отбор и систематизацию информации для определения альтернативных вариантов стратегических решений в проблемной ситуации, выделяет и оценивает риски возможных вариантов решений проблемной ситуации, вырабатывает стратегию действий по решению проблемной ситуации, осуществляет учёт требований законодательных и правовых актов РФ, регулирующих правовые отношения в сфере информационной безопасности и защиты государственной тайны, применяет цифровые технологии для решения проектных задач, выбирая оптимальный способ их решения, исходя из действующих правовых норм и имеющихся ресурсов и ограничений, обеспечивает выполнение проекта в соответствии с установленными целями, сроками и затратами, исходя из действующих правовых норм, имеющихся ресурсов и ограничений, в том числе с использованием цифровых инструментов, проводит контроль выполнения и оценивает эффективность реализации проекта на всех этапах его жизненного цикла, осознает свою роль в системе межличностного взаимодействия, анализирует стратегии поведения в группе, и особенности поведения разных групп людей, с которыми работает (взаимодействует), определяет статус и роль членов группы в системе межличностных отношений и учитывает на практике эти показатели, применяет методы командной работы, обеспечивает выполнение поставленных задач на основе мониторинга командной работы и своевременного реагирования на существенные отклонения, руководит выполнением поставленных задач на основе мониторинга командной работы и своевременного реагирования на существенные отклонения, руководствуется правилами деловой коммуникации в устной и письменной формах на государственном языке РФ и иностранном(ых) языке(ах), пользуется современными средствами деловой коммуникации на основе информационных технологий, осуществляет поиск и анализ требуемой информации в профессиональном взаимодействии, проводит оценку эффективности применяемых информационных технологий, решает профессиональные задачи с использованием современных коммуникационных технологий, проводит поиск необходимой информации в процессе решения стандартных коммуникативных задач на государственном(-ых) и иностранном(-ых) языках, проводит оценку эффективности применяемых коммуникативных технологий в профессиональном взаимодействии на государственном (-ых) и иностранном (-ых) языках, производит выбор оптимальных решений, учитывает культурные особенности и традиции различных социальных групп, этносов и конфессий, анализируя социальные ситуации взаимодействия, проявляет уважение к историческому наследию и социокультурным традициям различных социальных групп, опирающееся на знание этапов исторического развития России (включая основные события, основных исторических деятелей) в контексте мировой истории и ряда культурных традиций мира (в зависимости от среды и задач образования), включая мировые религии, философские и этические учения, выбирает формы, методы, приемы взаимодействия с различными социальными группами, учитывает культурные и религиозные традиции, при личном и массовом общении, определяет приемы конструктивного взаимодействия в ситуации общения, ставит цели в своей профессиональной деятельности и решает профессиональные задачи с учётом своих ресурсных возможностей и приоритетов, выбирает эффективные стратегии и тактики личностного и профессионального развития, пользуется методикой оценки эффективности применяемых методов решения поставленных задач в сфере своей профессиональной деятельности, оценивает эффективность использования времени и других ресурсов при решении поставленных задач в избранной сфере профессиональной деятельности, проводит критическую оценку эффективности использования своего времени и других ресурсов, при решении задач, поставленных в избранной сфере профессиональной деятельности, применяет методы решения задач моделирования и проектирования автоматизированных информационных систем и систем обеспечения информационной безопасности, разрабатывает и обосновывает критерии оценки эффективности проектируемой системы обеспечения информационной безопасности, разрабатывает актуальную модель угроз для автоматизированных информационных систем и

учитывает её положения при формировании требований технического задания на проектируемую систему обеспечения информационной безопасности, проводит разработку и обосновывает критерии оценки эффективности проектируемой системы обеспечения информационной безопасности, оценивает эффективность решений и анализирует показатели деятельности, определяет направления развития и проблем компьютерного моделирования сложных систем, разработке и исследовании системы защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасности, реализовывает типовые задачи средствами автоматизированного и ручного функционального тестирования, учитывает направления развития технологий проектирования информационных, автоматизированных и автоматических систем, управляет коллективом исполнителей и принимает управленческие решения, соблюдает правила построения оптимальной политики безопасности в соответствии с требованиями уровня безопасности, определяет стоимость и сроки реализации проекта, работает с нормативными правовыми актами в области информационной безопасности с технической и эксплуатационной документацией, оценивает различные инструменты в области проектирования и управления информационной безопасностью, соблюдает основы отечественных и зарубежных стандартов в области сертификации и аттестации объектов информатизации, учитывает основные угрозы безопасности информации и модели нарушителя в информационных системах, разрабатывает политики безопасности различных уровней, рассчитывает и разрабатывает положения о применимости механизмов контроля в контексте управления рисками информационной безопасности, соблюдает правила построения оптимальной политики безопасности в соответствии с требованиями уровня безопасности, определяет стоимость и сроки реализации проекта, работает с нормативными правовыми актами в области информационной безопасности с технической и эксплуатационной документацией, оценивает различные инструменты в области проектирования и управления информационной безопасностью, соблюдает основы отечественных и зарубежных стандартов в области сертификации и аттестации объектов информатизации, учитывает основные угрозы безопасности информации и модели нарушителя в информационных системах, разрабатывает политики безопасности различных уровней, рассчитывает и разрабатывает положения о применимости механизмов контроля в контексте управления рисками информационной безопасности, формулирует научную проблему, анализирует гипотезы, проводит выбор предмета, объекта, целей, задач исследования, создаёт эскизный, технический, рабочий проект, применяет технологии поиска, изучения, обобщения и систематизации научной информации, определяет комплекс мер для обеспечения безопасности информационных систем, составляет аналитические обзоры по вопросам обеспечения информационной безопасности систем, использует методы и средства анализа защищенности информационных систем, программные и аппаратные средства персонального компьютера для поиска и обработки информации, формулирует научную проблему, анализирует гипотезы, применяет методику создания технического задания и технического проекта при организации НИОКР, определяет порядок организации процесса исследования, методы построения оптимальных планов для научных экспериментов, оформляет научные публикации в соответствии с шаблоном IEEE, требованиями научных конференций, разрабатывает техническую документацию в соответствии с требованиями Единой системы конструкторской документации и Единой системы программной документации, анализирует получаемые результаты и формулирует выводы, выбирает и обосновывает критерии оценки защищенности открытых информационных систем, готовит научные доклады и статьи.

Оценка «неудовлетворительно» выставляется обучающему, если студент на низком уровне подбирает технологии поиска и критического анализа информации, использует методы системного подхода для решения поставленных задач с помощью цифровых и информационных технологий, организует личное цифровое пространство, осуществляет поиск, отбор и систематизацию информации для определения альтернативных вариантов стратегических решений в проблемной ситуации, выделяет и оценивает риски возможных

вариантов решений проблемной ситуации, вырабатывает стратегию действий по решению проблемной ситуации, осуществляет учёт требований законодательных и правовых актов РФ, регулирующих правовые отношения в сфере информационной безопасности и защиты государственной тайны, применяет цифровые технологии для решения проектных задач, выбирая оптимальный способ их решения, исходя из действующих правовых норм и имеющихся ресурсов и ограничений, обеспечивает выполнение проекта в соответствии с установленными целями, сроками и затратами, исходя из действующих правовых норм, имеющихся ресурсов и ограничений, в том числе с использованием цифровых инструментов, проводит контроль выполнения и оценивает эффективность реализации проекта на всех этапах его жизненного цикла, осознает свою роль в системе межличностного взаимодействия, анализирует стратегии поведения в группе, и особенности поведения разных групп людей, с которыми работает (взаимодействует), определяет статус и роль членов группы в системе межличностных отношений и учитывает на практике эти показатели, применяет методы командной работы, обеспечивает выполнение поставленных задач на основе мониторинга командной работы и своевременного реагирования на существенные отклонения, руководит выполнением поставленных задач на основе мониторинга командной работы и своевременного реагирования на существенные отклонения, руководствуется правилами деловой коммуникации в устной и письменной формах на государственном языке РФ и иностранном(ых) языке(ах), пользуется современными средствами деловой коммуникации на основе информационных технологий, осуществляет поиск и анализ требуемой информации в профессиональном взаимодействии, проводит оценку эффективности применяемых информационных технологий, решает профессиональные задачи с использованием современных коммуникационных технологий, проводит поиск необходимой информации в процессе решения стандартных коммуникативных задач на государственном(-ых) и иностранном(-ых) языках, проводит оценку эффективности применяемых коммуникативных технологий в профессиональном взаимодействии на государственном (-ых) и иностранном (-ых) языках, производит выбор оптимальных решений, учитывает культурные особенности и традиции различных социальных групп, этносов и конфессий, анализируя социальные ситуации взаимодействия, проявляет уважение к историческому наследию и социокультурным традициям различных социальных групп, опирающееся на знание этапов исторического развития России (включая основные события, основных исторических деятелей) в контексте мировой истории и ряда культурных традиций мира (в зависимости от среды и задач образования), включая мировые религии, философские и этические учения, выбирает формы, методы, приемы взаимодействия с различными социальными группами, учитывает культурные и религиозные традиции, при личном и массовом общении, определяет приемы конструктивного взаимодействия в ситуации общения, ставит цели в своей профессиональной деятельности и решает профессиональные задачи с учётом своих ресурсных возможностей и приоритетов, выбирает эффективные стратегии и тактики личностного и профессионального развития, пользуется методикой оценки эффективности применяемых методов решения поставленных задач в сфере своей профессиональной деятельности, оценивает эффективность использования времени и других ресурсов при решении поставленных задач в избранной сфере профессиональной деятельности, проводит критическую оценку эффективности использования своего времени и других ресурсов, при решении задач, поставленных в избранной сфере профессиональной деятельности, применяет методы решения задач моделирования и проектирования автоматизированных информационных систем и систем обеспечения информационной безопасности, разрабатывает и обосновывает критерии оценки эффективности проектируемой системы обеспечения информационной безопасности, разрабатывает актуальную модель угроз для автоматизированных информационных систем и учитывает её положения при формировании требований технического задания на проектируемую систему обеспечения информационной безопасности, проводит разработку и обосновывает критерии оценки эффективности проектируемой системы обеспечения информационной безопасности, оценивает

эффективность решений и анализирует показатели деятельности, определяет направления развития и проблем компьютерного моделирования сложных систем, разработке и исследовании системы защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасности, реализовывает типовые задачи средствами автоматизированного и ручного функционального тестирования, учитывает направления развития технологий проектирования информационных, автоматизированных и автоматических систем, управляет коллективом исполнителей и принимает управленческие решения, соблюдает правила построения оптимальной политики безопасности в соответствии с требованиями уровня безопасности, определяет стоимость и сроки реализации проекта, работает с нормативными правовыми актами в области информационной безопасности с технической и эксплуатационной документацией, оценивает различные инструменты в области проектирования и управления информационной безопасности, соблюдает основы отечественных и зарубежных стандартов в области сертификации и аттестации объектов информатизации, учитывает основные угрозы безопасности информации и модели нарушителя в информационных системах, разрабатывает политики безопасности различных уровней, рассчитывает и разрабатывает положения о применимости механизмов контроля в контексте управления рисками информационной безопасности, соблюдает правила построения оптимальной политики безопасности в соответствии с требованиями уровня безопасности, определяет стоимость и сроки реализации проекта, работает с нормативными правовыми актами в области информационной безопасности с технической и эксплуатационной документацией, оценивает различные инструменты в области проектирования и управления информационной безопасности, соблюдает основы отечественных и зарубежных стандартов в области сертификации и аттестации объектов информатизации, учитывает основные угрозы безопасности информации и модели нарушителя в информационных системах, разрабатывает политики безопасности различных уровней, рассчитывает и разрабатывает положения о применимости механизмов контроля в контексте управления рисками информационной безопасности, формулирует научную проблему, анализирует гипотезы, проводит выбор предмета, объекта, целей, задач исследования, создаёт эскизный, технический, рабочий проект, применяет технологии поиска, изучения, обобщения и систематизации научной информации, определяет комплекс мер для обеспечения безопасности информационных систем, составляет аналитические обзоры по вопросам обеспечения информационной безопасности систем, использует методы и средства анализа защищенности информационных систем, программные и аппаратные средства персонального компьютера для поиска и обработки информации, формулирует научную проблему, анализирует гипотезы, применяет методику создания технического задания и технического проекта при организации НИОКР, определяет порядок организации процесса исследования, методы построения оптимальных планов для научных экспериментов, оформляет научные публикации в соответствии с шаблоном IEEE, требованиями научных конференций, разрабатывает техническую документацию в соответствии с требованиями Единой системы конструкторской документации и Единой системы программной документации, анализирует получаемые результаты и формулирует выводы, выбирает и обосновывает критерии оценки защищенности открытых информационных систем, готовит научные доклады и статьи.

Студент, не сдавший государственный междисциплинарный экзамен, не имеет права быть допущенным к защите выпускной квалификационной работы. Студент, не прошедший итоговые аттестационные испытания, отчисляется из вуза.

8.3. Описание шкалы оценивания

Государственный экзамен оценивается по 5-балльной системе.

УТВЕРЖДАЮ

Декан факультета математики и
компьютерных наук имени
профессора Н.И.Червякова
_____ Т. А. Грובה

**ТРЕБОВАНИЯ К ВЫПУСКНЫМ КВАЛИФИКАЦИОННЫМ РАБОТАМ
(ПО ВИДАМ) И ПОРЯДКУ ИХ ВЫПОЛНЕНИЯ**

Направление подготовки	10.04.01 Информационная безопасность
Направленность (профиль)/специализация	Информационная безопасность киберфизических систем
Год начала обучения	2026
Форма обучения	очная
Реализуется в семестре	4

РАЗРАБОТАНО:

Доцент кафедры организации и технологии
защиты информации
Бисюков Виктор Михайлович

Ставрополь, 2026

1. Введение

Выпускная квалификационная работа - это квалификационное, комплексное, научное исследование, являющееся заключительным этапом обучения студентов по профессиональной программе.

По своему содержанию ВКР представляет собой самостоятельно выполненную квалификационную, комплексную (научную работу) в области информационной безопасности, имеющую научное, методическое или практическое значение.

ВКР относится к разряду учебно-исследовательских работ. Выполнение такой работы служит свидетельством того, что ее автор научился самостоятельно решать профессиональные задачи по направлению «Информационная безопасность». Выпускная квалификационная работа в соответствии с магистерской программой выполняется в виде магистерской диссертации в период прохождения практики и выполнения научно-исследовательской работы и представляет собой самостоятельную и логически завершенную выпускную квалификационную работу, связанную с решением задач того вида или видов деятельности, к которым готовится магистр (проектная научно-исследовательская научно-педагогическая организационно-управленческая).

Рекомендуется применять сквозное проектирование, при котором тема (или часть ее) последовательно разрабатывается в курсовых, а затем и в магистерских диссертациях с постепенным ее расширением и углублением.

ВКР выполняется под руководством научного руководителя – ведущего преподавателя кафедры организации и технологии защиты информации.

ВКР считаются выполненной по реальной тематике, если:

- имеется заявка предприятия на выполнение ВКР с указанием тематики или запрос предприятия на полную или частичную передачу материалов магистерской диссертации для их реализации,
- имеется заявка на патент или положительное решение о его выдаче, удостоверение на рационализаторское предложение, суть которых отражена в основной части магистерской диссертации,
- решение магистерской диссертации является технической разработкой запатентованной идеи,
- материалы магистерской диссертации используются в хозяйственной или государственной научно-исследовательской работе – имеется подтверждение апробации результатов и выводов работы в виде докладов на научных конференциях, публикаций в журналах, сборниках научных статей или внедрение в производство.

Работа над ВКР может выполняться студентом на предприятии, в организации, в научных и проектно-конструкторских и других учреждениях и непосредственно в Университете.

Защита ВКР является основанием для присуждения выпускнику степени (квалификации) – магистр.

Исходными данными для выполнения ВКР являются:

- результаты предпроектного обследования существующей на предприятии (организации, учреждении и фирме) информационной системы (подсистемы), представленные в отчетах по производственной и преддипломной практике студента,

- формы документов, используемых на предприятии (организации, учреждении и фирме),
- прайс-листы, данные о поставщиках, данные о клиентах и другие документы, необходимые для решения задачи проектирования.

Тематика ВКР разрабатывается выпускающей кафедрой, рассматривается и утверждается Ученым советом факультета математики и компьютерных наук имени профессора Н.И.Червякова и должна быть направлена на решение профессиональных задач.

Научный руководитель ВКР:

- выдает задание для выполнения работы,
- оказывает помощь в разработке календарного графика работы на весь период выполнения ВКР,
- формирует программу работы магистра,
- рекомендует магистру необходимую основную литературу, справочные и архивные материалы, типовые проекты и другие источники по теме,
- устанавливает расписание консультаций, при проведении которых осуществляет текущий контроль соблюдения магистром календарного графика выполнения ВКР,
- устанавливает объем всех разделов ВКР и координирует работу студента.

2. Цели и задачи выпускной квалификационной работы

Выполнение ВКР имеет следующие цели и задачи:

- систематизация, закрепление, расширение теоретических знаний и практических умений по специальности (направлению) и использование их при решении профессиональных задач,
- развитие навыков самостоятельной научной работы и овладение методикой построения экспериментальных исследований,
- подготовка студентов к научно-исследовательской, учебно-воспитательной и экспертно-аналитической работе в условиях реальной профессиональной деятельности,
- завершение формирования общекультурных и профессиональных компетенций выпускника.

3. Перечень компетенций, уровень сформированности которых должен быть проверен в ходе защиты выпускной квалификационной работы

ПК-1	Способен проводить исследования и анализ информационных процессов защиты информации в киберфизических системах
ПК-2	Способен проектировать и реализовывать политику безопасности вычислительных сетей в киберфизических системах
ПК-3	Способен разрабатывать предложения по совершенствованию системы управления информационной безопасностью киберфизических систем
ПК-4	Способен оценивать уровень защищенности киберфизических систем и применять решения по обеспечению их информационной безопасности

4. Структура и объем выпускной квалификационной работы (по видам), в т. ч. объем каждого из разделов выпускной квалификационной работы

4.1 Общая структура выпускной квалификационной работы

Дипломная работа по направлению 10.04.01 (магистратура) имеет следующую обязательную структуру:

Титульный лист;

Задание на выпускную квалификационную работу (дипломную работу);

Календарный план;

Реферат (аннотация), в т.ч. на иностранном языке (при необходимости);

Содержание (оглавление);

Введение. Объём введения — 3–5 страниц;

Основная часть (не менее трёх разделов). Раздел 1 — Аналитическая часть. Раздел завершается постановкой задачи исследования. Объём — 15–25 страниц. Раздел 2 — Проектная (исследовательская) часть. Объём — 20–35 страниц. Раздел 3 — Экономическая и эксплуатационная часть. Объём — 10–15 страниц;

Заключение. Объём — 2–4 страницы;

Список использованных источников. Минимальное количество источников — 30, в том числе не менее 5 на иностранном языке;

Приложения (при необходимости).

Объём ВКР 50-60 страниц.

Содержание выпускной квалификационной работы (по видам), в т. ч. содержание каждого из разделов, включенных в структуру выпускной квалификационной работы

5.1 Введение

Введение содержит: обоснование актуальности темы в контексте современных угроз информационной безопасности; характеристику объекта и предмета исследования; цель и задачи работы; методологическую основу; теоретическую и практическую значимость; структуру работы.

5.2 Раздел 1 — Аналитическая часть

Раздел 1 является аналитическим и включает:

обзор и анализ нормативно-правовой базы в области защиты информации, применимой к объекту исследования (ФЗ-149, ФЗ-152, ФЗ-187, требования ФСТЭК России, ФСБ России и др.);

описание объекта информатизации: состав, структура, функциональное назначение, категория защищаемых ресурсов (сведения, составляющие государственную тайну / конфиденциальную информацию / персональные данные);

анализ актуальных угроз информационной безопасности: разработку или актуализацию модели угроз и нарушителя в соответствии с методологией ФСТЭК России;

анализ существующей системы защиты информации на объекте: выявление недостатков и уязвимостей с точки зрения обеспечения конфиденциальности, целостности и доступности защищаемых ресурсов;

обзор и сравнительный анализ существующих методов, средств и технологий защиты, применимых к исследуемой проблеме; патентный поиск.

5.3 Раздел 2 — Проектная (исследовательская) часть

Раздел 2 является основным и содержит разработанные (усовершенствованные) технические и/или организационные решения. В зависимости от темы Раздел включает:

- разработку технического проекта системы (подсистемы) обеспечения информационной безопасности объекта информатизации: состав, структура, функциональная схема, обоснование выбранных технических мер защиты;
- разработку или актуализацию комплекта организационно-распорядительной документации: политики безопасности, регламентов, инструкций, положений о защите информации;
- разработку средств защиты от НСД (программных, аппаратных, криптографических) с описанием алгоритмов, схем и результатов тестирования (ПК-1, ПК-2, ПК-3);
- формирование требований к защите информации в проектируемой или модернизируемой автоматизированной системе (ПК-4);
- моделирование процессов защиты информации, разработку математических моделей или алгоритмов, обоснование их корректности;
- обоснование проектных решений с точки зрения обеспечения конфиденциальности, целостности и доступности защищаемых ресурсов.

5.4 Раздел 3 — Экономическая и эксплуатационная часть

Раздел 3 содержит:

техничко-экономическое обоснование разработанных решений: расчёт затрат на создание и внедрение системы защиты информации, оценку экономического ущерба от нарушений ИБ и эффективности предложенных мер;

рекомендации по внедрению (вводу в эксплуатацию) системы защиты информации: порядок аттестации объекта информатизации, требования к персоналу, эксплуатационную документацию;

оценку рисков информационной безопасности после внедрения предложенных решений (сравнительный анализ до/после);

вопросы безопасности и охраны труда при эксплуатации средств вычислительной техники и средств защиты информации (при необходимости).

5.5 Заключение

Заключение содержит: обобщённые выводы по результатам работы; степень достижения поставленной цели и решения задач; оценку научной новизны и практической значимости полученных результатов; направления дальнейших исследований.

5.6 Список использованных источников

Список оформляется в соответствии с ГОСТ 7.32-2017 «Отчёт по научно-исследовательской работе. Структура и правила оформления», актуальных публикаций в рецензируемых научных изданиях.

6. Оформление выпускной квалификационной работы (по видам)

6.1 Общие требования к оформлению выпускных квалификационных работ

Контроль за выполнением требований к оформлению ВКР (соответствие нормам и требованиям действующих государственных, международных, отраслевых стандартов и других нормативных документов, оформление текста, списка литературы, чертежей и т.д.) осуществляет нормоконтролер.

Нормоконтролерами могут назначаться высококвалифицированные преподаватели выпускающей кафедры, также функции нормоконтролера может выполнять сам руководитель ВКР. При проведении нормоконтроля следует руководствоваться указателями (каталогами, перечнями) государственных, международных и отраслевых стандартов, технических условий, действующими нормативными документами, распространяющимися на объект стандартизации, терминологическими словарями (справочниками, сборниками), картотеками внедрения нормативных документов, таблицами систематизации и др.

Нормоконтролер имеет право:

- возвращать ВКР в случаях несоответствия требованиям, небрежного выполнения, отсутствия необходимых подписей, отсутствия документов, на которые имеются ссылки в работе и т.д.,

- требовать от студента разъяснений и дополнительных материалов по возникшим при проверке вопросам,

- не подписывать ВКР в случаях невыполнения требований.

Выпускные квалификационные работы должны оформляться:

- по инженерным направлениям подготовки и специальностям: ГОСТ 2.105-95. Общие требования к текстовым документам, ГОСТ 2.106-96. Текстовые документы, ГОСТ 2.104-68. Основные надписи, Единая система конструкторской документации, Единая система технологической документации, Единая система программной документации, ГОСТ 7.1-2003. Библиографическая запись. Библиографическое описание, ГОСТ 7.82-2001. Библиографическая запись. Библиографическое описание электронных ресурсов, ГОСТ Р 7.0.5-2008. Библиографическая ссылка. Общие требования и правила составления, ГОСТ 7.80-2000. Библиографическая запись. Заголовок. Общие требования и правила составления,

- по остальным направлениям подготовки и специальностям - по ГОСТ 7.32-2001. Отчет по научно-исследовательской работе. Структура и правила оформления, ГОСТ 7.1-2003. Библиографическая запись. Библиографическое описание, ГОСТ 7.82-2001. Библиографическая запись. Библиографическое описание электронных ресурсов, ГОСТ Р 7.0.5-2008. Библиографическая ссылка. Общие требования и правила составления, ГОСТ 7.80-2000. Библиографическая запись. Заголовок. Общие требования и правила составления,

- в соответствии с Требованиями к выпускным квалификационным работам и порядку их выполнения, разработанными выпускающими кафедрами в соответствии с вышеперечисленными ГОСТами и нормативно-технической документацией по направлению.

Текст ВКР выполняют с использованием компьютера на одной стороне листа белой бумаги, **формата А4, шрифт - Times New Roman 14-го размера, межстрочный интервал - 1,5.**

Полужирный шрифт применяют только для заголовков разделов и подразделов, заголовков структурных элементов. Использование курсива допускается для обозначения терминов (например, *in vivo*, *in vitro*) и иных объектов и терминов на латыни.

Для акцентирования внимания может применяться выделение текста с помощью шрифта иного начертания, чем шрифт основного текста, но того же кегля и гарнитуры.

Разрешается для написания определенных терминов, формул, теорем применять шрифты разной гарнитуры.

Текст отчета следует печатать, соблюдая следующие размеры полей: **левое — 30 мм. правое — 15 мм. верхнее и нижнее — 20 мм.** Абзацный отступ должен быть одинаковым по всему тексту отчета и равен **1,25 см.**

Наименования структурных элементов ВКР: «СОДЕРЖАНИЕ», «ПЕРЕЧЕНЬ СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ», «ВВЕДЕНИЕ», «ЗАКЛЮЧЕНИЕ», «СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ», «ПРИЛОЖЕНИЕ» служат заголовками структурных элементов отчета.

Заголовки структурных элементов следует располагать в середине строки без точки в конце, прописными буквами, не подчеркивая. Каждый структурный элемент и каждый раздел основной части отчета начинают с новой страницы.

Основную часть ВКР следует делить на разделы, подразделы и пункты. Пункты при необходимости могут делиться на подпункты. Разделы и подразделы отчета должны иметь заголовки. Пункты и подпункты, как правило, заголовков не имеют.

Заголовки разделов и подразделов основной части отчета следует начинать с абзацного отступа и размещать после порядкового номера, **печатать с прописной буквы, полужирным шрифтом, не подчеркивать, без точки в конце.** Пункты и подпункты могут иметь только порядковый номер без заголовка, начинающийся с абзацного отступа.

Если заголовок включает несколько предложений, их разделяют точками. Переносы слов в заголовках не допускаются.

Страницы ВКР следует нумеровать арабскими цифрами, соблюдая сквозную нумерацию по всему тексту, включая приложения. Номер страницы проставляется в центре нижней части страницы без точки. Приложения, которые приведены в ВКР и имеющие собственную нумерацию, допускается не перенумеровать.

Титульный лист текстового документа включают в общую нумерацию страниц. Номер страницы на титульном листе не проставляют.

Разделы должны иметь порядковые номера в пределах всей ВКР, обозначенные арабскими цифрами без точки и расположенные с абзацного отступа. Подразделы должны иметь нумерацию в пределах каждого раздела. Номер подраздела состоит из номеров раздела и подраздела, разделенных точкой. В конце номера подраздела точка не ставится. Разделы, как и подразделы, могут состоять из одного или нескольких пунктов.

Если ВКР имеет подразделы, то нумерация пунктов должна быть в пределах подраздела и номер пункта должен состоять из номеров раздела, подраздела и пункта, разделенных точками. Каждый раздел должен заканчиваться выводами.

Заголовок разделов, подразделов и пунктов следует печатать с абзацного отступа, с прописной буквы, без точки в конце, не подчеркивая. Переносы слов в заголовках не допускаются. Если заголовок состоит из двух предложений, их разделяют точкой.

Между разделами и подразделами, подразделами и текстом оставляют отступ 12 пт. Пример:

1 Анализ структуры, деятельности и информационных ресурсов предприятия.
Обоснование направлений исследования

1.1 Анализ структуры предприятия

1.2 Анализ деятельности предприятия

1.2.1 Анализ нормативных документов, регламентирующих деятельность отделов предприятия

1.2.1.1 Анализ нормативных документов дирекции предприятия

1.3 Обоснование направления исследования

2 Разработка рекомендаций по построению системы защиты информации в информационной системе предприятия

2.1 Оценка риска информационной системы предприятия

2.1 Оценка риска информационной системы предприятия

Если раздел или подраздел состоит из одного пункта, он также нумеруется. Если текст документа подразделяется только на пункты, они нумеруются порядковыми номерами в пределах документа.

Пункты, при необходимости, могут быть разбиты на подпункты, которые должны иметь порядковую нумерацию в пределах каждого пункта, например 4.2.1, 4.2.1.1, 4.2.1.2, 4.2.2 и т. д. Между подпунктами и текстом интервалы не оставляются. Внутри пунктов или подпунктов могут быть приведены перечисления.

Перед каждым перечислением следует ставить **тире** или, при необходимости ссылки в тексте документа на одно из перечислений, вместо тире ставят строчные буквы русского алфавита со скобкой, начиная с буквы «а» (за исключением букв ё, э, й, о, ч. ъ, ы, ь). Простые перечисления отделяются запятой, сложные — точкой с запятой.

При наличии конкретного числа перечислений допускается перед каждым элементом перечисления ставить арабские цифры, после которых ставится скобка.

Перечисления приводятся с абзацного отступа в столбик.

Пример 1

Информационно-сервисная служба для обслуживания удаленных пользователей включает следующие модули:

- удаленный заказ,
- виртуальная справочно служба,
- виртуальный читальный зал,

Пример 2

Работа по оцифровке включала следующие технологические этапы:

- а) первичный осмотр и структурирование исходных материалов.
- б) сканирование документов,
- в) обработка и проверка полученных образов.
- г) структурирование оцифрованного массива.
- д) выходной контроль качества массивов графических образов.

Пример 3

Камеральные и лабораторные исследования включали разделение всего выявленного видового состава растений на четыре группы по степени использования их копытными:

- 1) случайный корм.
- 2) второстепенный корм.
- 3) дополнительный корм.
- 4) основной корм.

Пример 4

Разрабатываемое сверхмощное устройство можно будет применять в различных отраслях реального сектора экономики:

- в машиностроении:

- 1) для очистки отливок от формовочной смеси,
- 2) для очистки лопаток турбин авиационных двигателей,
- 3) для холодной штамповки из листа,

- в ремонте техники:

- 1) устранение наслоений на внутренних стенках труб,
- 2) очистка каналов и отверстий небольшого диаметра от грязи.

Содержание включает введение, наименование всех разделов и подразделов, пунктов (если они имеют наименование), заключение, список использованных источников и наименования приложений с указанием номеров страниц, с которых начинаются эти элементы ВКР.

В элементе «СОДЕРЖАНИЕ» приводят наименования структурных элементов работы, порядковые номера и заголовки разделов, подразделов (при необходимости — пунктов) основной части работы, обозначения и заголовки ее приложений (при наличии приложений). После заголовка каждого элемента ставят отточие и приводят номер страницы работы, на которой начинается данный структурный элемент.

Обозначения подразделов приводят после абзацного отступа, равного двум знакам, относительно обозначения разделов. Обозначения пунктов приводят после абзацного отступа, равного четырем знакам относительно обозначения разделов.

При необходимости продолжение записи заголовка раздела, подраздела или пункта на второй (последующей) строке выполняют, начиная от уровня начала этого заголовка на первой строке, а продолжение записи заголовка приложения — от уровня записи обозначения этого приложения.

6.2 Изложение текста

Текст документа должен быть кратким, четким и не допускать различных толкований.

При изложении обязательных требований в тексте должны применяться слова "должен", "следует", "необходимо", "требуется, чтобы", "разрешается только", "не допускается", "запрещается", "не следует". При изложении других положений следует применять слова - "могут быть", "как правило", "при необходимости", "может быть", "в случае" и т.д.

При этом допускается использовать повествовательную форму изложения текста документа, например "применяют", "указывают" и т.п.

В тексте должны применяться научно-технические термины, обозначения и определения, установленные соответствующими стандартами, а при их отсутствии — общепринятые в научно-технической литературе.

В тексте не допускается:

- применять обороты разговорной речи, техницизмы, профессионализмы,

- применять для одного и того же понятия различные научно-технические термины, близкие по смыслу (синонимы), а также иностранные слова при наличии равнозначных слов и терминов на русском языке,

- сокращать обозначения единиц физических величин, если они употребляются без цифр, за исключением единиц физических величин в головках и боковиках таблиц, в расшифровках буквенных обозначений, входящих в формулы и рисунки, применять математический знак минус (-) перед отрицательными значениями величин (следует писать слово «минус»),

- применять знак «Ø» для обозначения диаметра следует писать слово «диаметр»). При указании размера или предельного отклонения диаметра на чертежах, помещенных в тексте документа, перед размерным числом следует писать знак «Ø»,

- применять без числовых значений математические знаки, например, > (больше), < (меньше), = (равно), ≠ (не равно), а также знака № (номер), % (процент), применять индексы стандартов без регистрирующего номера, перечень допускаемых сокращений слов установлен в ГОСТ 2.316, ГОСТ 7.12, в тексте следует применять стандартизованные единицы физических величин, их наименование и обозначение, установленные в ГОСТ 8.417,

- если в тексте дипломной работы приводится диапазон числовых значений физической величины, то обозначение единицы физической величины указывается, после последнего числового значения диапазона.

Пример: От 1 до 5 мм. Или от плюс 10 до минус 400 С.

Недопустимо отделять единицу физической величины от числового значения (переносить их на разные строки или страницы), кроме единиц физических величин, помещенных в таблицах, выполненных машинописным способом.

6.3 Формулы и уравнения

Уравнения и формулы следует выделять из текста в отдельную строку. Выше и ниже каждой формулы или уравнения должно быть оставлено не менее одной свободной строки. Если уравнение не уместится в одну строку, то оно должно быть перенесено после знака равенства (=) или после знаков плюс (+), минус (-), умножения (x), деления (:), или других математических знаков, причем знак в начале следующей строки повторяют. При переносе формулы на знаке, символизирующем операцию умножения, применяют знак «X».

Пояснение значений символов и числовых коэффициентов следует приводить непосредственно под формулой в той же последовательности, в которой они даны в формуле. Значение каждого символа и числового коэффициента необходимо приводить с новой строки. Первую строку пояснения начинают со слова «где» без двоеточия с абзаца.

Формулы в работе следует располагать посередине строки и обозначать порядковой нумерацией в пределах всей работы арабскими цифрами в круглых скобках в крайнем правом положении на строке. Одну формулу обозначают (1).

Пример:

$$PS = \langle F, Z, I \rangle, \quad (1)$$

где F - рабочая память системы (называемая также базой данных), содержащая текущие данные (элементы рабочей памяти),

Z - база знаний, содержащая множество продукций (правил вида: "условие → действие"),

I - интерпретатор (решатель), реализующий процедуры вывода.

Ссылки в работе на порядковые номера формул приводятся в скобках: в формуле (1).

Формулы, помещаемые в приложениях, должны нумероваться отдельной нумерацией арабскими цифрами в пределах каждого приложения с добавлением перед каждой цифрой обозначения приложения, например, формула (B.1).

Допускается нумерация формул в пределах раздела. В этом случае номер формулы состоит из номера раздела и порядкового номера формулы, разделенных точкой, например (3.1).

Формулы, следующие одна за другой и не разделенные текстом, разделяют запятой.

6.4 Иллюстрации

Иллюстрации (чертежи, графики, схемы, компьютерные распечатки, диаграммы, фотоснимки) следует располагать в ВКР непосредственно после текста, в котором они упоминаются впервые, или на следующей странице. Иллюстрации могут быть в компьютерном исполнении, в том числе и цветные. На все иллюстрации должны быть даны ссылки в дипломной работе. При ссылке необходимо писать слово «рисунок» и его номер, например: «в соответствии с рисунком 2» и т. д.

Чертежи, графики, диаграммы, схемы, иллюстрации, помещаемые в ВКР, должны соответствовать требованиям государственных стандартов Единой системы конструкторской документации (ЕСКД).

Допускается выполнение чертежей, графиков, диаграмм, схем посредством использования компьютерной печати.

Фотоснимки размером меньше формата А4 должны быть наклеены на стандартные листы белой бумаги.

Иллюстрации, за исключением иллюстрации приложений, следует нумеровать арабскими цифрами сквозной нумерацией. Если рисунок один, то он обозначается «Рисунок 1». Слово «Рисунок» и его наименование располагают посередине строки (Рисунок 1).

Пример:

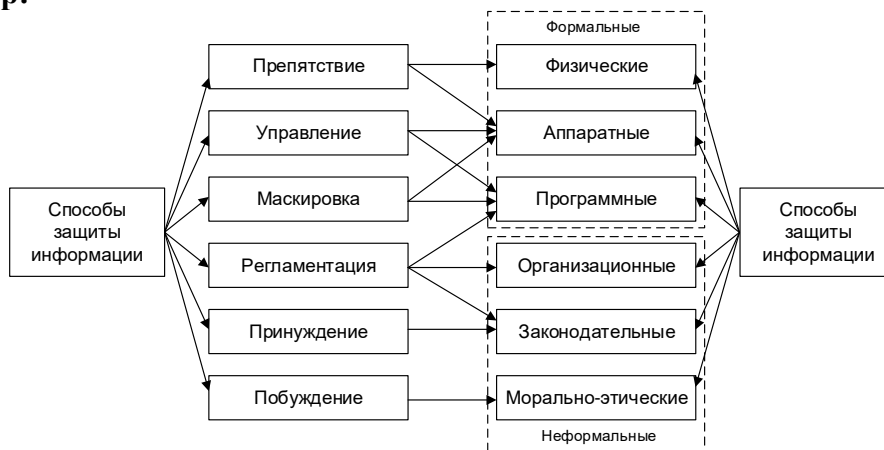


Рисунок 1 – Основные характеристики системы защиты

Иллюстрации каждого приложения обозначают отдельной нумерацией арабскими цифрами с добавлением перед цифрой обозначения приложения: Рисунок А.3.

Допускается нумеровать иллюстрации в пределах раздела. В этом случае номер иллюстрации состоит из номера раздела и порядкового номера иллюстрации, разделенных точкой: Рисунок 2.1.

Иллюстрации при необходимости могут иметь наименование и пояснительные данные (подрисуночный текст). Слово «Рисунок», его номер и через тире наименование помещают после пояснительных данных и располагают в центре под рисунком без точки в конце.

Если наименование рисунка состоит из нескольких строк, то его следует записывать через один межстрочный интервал. Наименование рисунка приводят с прописной буквы без точки в конце. Перенос слов в наименовании графического материала не допускается.

6.5 Приложения

Приложения могут включать: графический материал, таблицы не более формата А3, расчеты, описания алгоритмов и программ.

Приложение оформляют одним из следующих 2-х способов:

- 1) как продолжение данной работы на последующих его листах,
- 2) в виде самостоятельного документа.

В тексте ВКР на все приложения должны быть даны ссылки. Приложения располагают в порядке ссылок на них в тексте работы.

Каждое приложение следует размещать с новой страницы с указанием в центре верхней части страницы слова «ПРИЛОЖЕНИЕ».

Приложение должно иметь заголовок, который записывают с прописной буквы, полужирным шрифтом, отдельной строкой по центру без точки в конце.

Приложения обозначают прописными буквами кириллического алфавита, начиная с А. за исключением букв Ё. З. Й. О. Ч. Ъ. Ы. Ь. После слова «ПРИЛОЖЕНИЕ» следует буква, обозначающая его последовательность. Допускается обозначение приложений буквами латинского алфавита, за исключением букв I и O.

В случае полного использования букв кириллического или латинского алфавита допускается обозначать приложения арабскими цифрами.

Если в работе одно приложение, оно обозначается «ПРИЛОЖЕНИЕ А».

Приложения, как правило, выполняют на листах формата А4. Допускается оформление приложения на листах формата А3.

Текст каждого приложения при необходимости может быть разделен на разделы, подразделы, пункты, подпункты, которые нумеруют в пределах каждого приложения. Перед номером ставится обозначение этого приложения.

Приложения должны иметь общую с остальной частью отчета сквозную нумерацию страниц.

Все приложения должны быть перечислены в содержании ВКР (при наличии) с указанием их обозначений, статуса и наименования.

Пример:

ПРИЛОЖЕНИЕ А
(обязательное)

6.6 Таблицы

Таблицы применяют для наглядности и удобства сравнения показателей. Название таблицы, при его наличии, должно отражать ее содержание, быть точным, кратким. Наименование таблицы приводят с прописной буквы без точки в конце. Слово "Таблица" указывают один раз слева над первой частью таблицы, над другими частями пишут слова "Продолжение таблицы" с указанием номера (обозначения) таблицы. При переносе части таблицы название помещают только над первой частью таблицы.

Если наименование таблицы занимает две строки и более, то его следует записывать через один межстрочный интервал.

При делении таблицы на части допускается ее головку или боковик заменять соответственно номерами граф и строк. При этом нумеруют арабскими цифрами графы и (или) строки первой части таблицы.

Таблицу следует располагать в дипломной работе непосредственно после текста, в котором она упоминается впервые, или на следующей странице.

Допускается помещать таблицу вдоль длинной стороны листа документа. На все таблицы должны быть ссылки в отчете. При ссылке следует писать слово «таблица» с указанием ее номера.

Таблицу с большим количеством строк допускается переносить на другой лист (страницу). При переносе части таблицы на другой лист (страницу) слово «Таблица» и номер ее указывают слева над первой частью таблицы, над другими частями пишут «Продолжение таблицы 1».

Цифровой материал, как правило, оформляют в виде таблиц в соответствии с рисунком 2.



Рисунок 2 – Общий вид таблицы

Если цифровые или иные данные в какой-либо строке таблицы не приводят, то в ней ставят прочерк.

Таблицы, за исключением таблиц приложений, следует нумеровать арабскими цифрами сквозной нумерацией.

Таблицы каждого приложения обозначаются отдельной нумерацией арабскими цифрами с добавлением перед цифрой обозначения приложения. Если в работе одна таблица, она должна быть обозначена «Таблица 1» или «Таблица А.1» (если она приведена в приложении А).

Заголовки граф и строк таблицы следует писать с прописной буквы в единственном числе, а подзаголовки граф - со строчной буквы, если они составляют одно предложение с заголовком, или с прописной буквы, если они имеют самостоятельное значение. В конце

заголовков и подзаголовков таблиц точки не ставятся. Названия заголовков и подзаголовков таблиц указывают в единственном числе.

Таблицы слева, справа и снизу, как правило, ограничивают линиями. Допускается применять размер шрифта в таблице меньший, чем в тексте.

Разделять заголовки и подзаголовки боковика и граф диагональными линиями не допускается. Заголовки граф выравнивают по центру, а заголовки строк — по левому краю. При необходимости допускается перпендикулярное расположение заголовков граф.

Если строки или графы таблицы выходят за формат страницы, ее делят на части, помещая одну часть под другой или рядом, при этом в каждой части таблицы повторяют ее головку и боковик. Оформление таблиц в дипломной работе должно соответствовать ГОСТ 1.5 и ГОСТ 2.105.

Пример:

Таблица 1 – Результаты структурирования информации

№ элемента информации	Наименование элемента информации	Гриф конфиденциальности информации	Цена информации	Наименование источника информации	№ элемента информации
1	2	3	4	5	6

Продолжение таблицы 1

1	2	3	4	5	6

Графическая часть ВКР (чертежи, схемы и т. п.) выполняется с соблюдением соответствующих государственных стандартов. Каждое приложение должно начинаться с нового листа с указанием сверху листа по центру слова «Приложение» и иметь тематический заголовок.

При оформлении ВКР, на внутренней стороне второго листа обложки приклеивается конверт, формата А5, в который помещаются:

- отзыв руководителя,
- рецензия,
- заявка на выполнение и Акт о внедрении результатов ВКР.

7. Порядок выполнения выпускной квалификационной работы (по видам) и порядок подготовки выпускной квалификационной работы к защите (по видам)

Организацию и контроль выполнения ВКР осуществляют выпускающая кафедра, дирекция факультета (филиала), декан факультета (при наличии).

Перечень тем выпускных квалификационных работ, предлагаемых обучающимся (далее - перечень тем), ежегодно определяется на заседаниях выпускающих кафедр, утверждается Ученым советом факультета (филиала) и доводится до сведения обучающихся не позднее, чем за шесть месяцев до даты начала государственной итоговой аттестации.

Темы выпускных квалификационных работ должны быть актуальными, соответствовать профилю направления подготовки или специальности, учитывать отраслевую специфику и направленность деятельности СКФУ, современное состояние и перспективы развития науки.

Обучающемуся предоставляется право выбора темы выпускной квалификационной работы. По письменному заявлению обучающегося (нескольких обучающихся, выполняющих выпускную квалификационную работу совместно) выпускающая кафедра может в установленном порядке предоставить обучающемуся (обучающимся) возможность подготовки и защиты выпускной квалификационной работы по теме, предложенной обучающимся (обучающимися), в случае обоснованности целесообразности ее разработки для практического применения в соответствующей области профессиональной деятельности или на конкретном объекте профессиональной деятельности.

Заведующие выпускающими кафедрами СКФУ не позднее, чем за 15 календарных дней до начала преддипломной практики на основании личных заявлений обучающихся закрепляют за обучающимся (несколькими обучающимися) на заседании кафедры темы выпускных квалификационных работ, руководителей из числа профессоров, доцентов выпускающей кафедры и, в исключительных случаях, в соответствии с ходатайством кафедры и решением Ученого совета факультета (филиала), старших преподавателей, имеющих стаж работы в Университете не менее 5 лет или имеющих стаж работы в соответствующей профессиональной области не менее 3 лет. По предложению руководителя ВКР, в случае необходимости, выпускающей кафедре предоставляется право приглашать консультантов (соруководителей) по отдельным разделам работы, за счет нормы времени, отведенного на руководство ВКР. При выполнении ВКР по междисциплинарной тематике в качестве консультантов (соруководителей) могут назначаться профессора и высококвалифицированные преподаватели других кафедр Университета, а также научные работники и специалисты профильных учреждений региона, являющиеся внешними совместителями.

За 7 календарных дней до начала преддипломной практики студентам выпускных курсов распоряжением директора факультета (филиала) на основании представлений заведующих выпускающими кафедрами утверждаются темы выпускных квалификационных работ (с указанием вида выпускной квалификационной работы), руководители (консультанты) с указанием их ученой степени, звания и должности.

Выпускающая кафедра обеспечивает студентов Требованиями к выпускным квалификационным работам и порядку их выполнения, в которых содержатся:

- требования к структуре, содержанию, объему и оформлению выпускных квалификационных работ применительно к направлению (специальности), а также порядку их выполнения,

- критерии оценки выпускных квалификационных работ.

Закрепленная за студентом ВКР выполняется в соответствии с заданием по изучению объекта и предмета исследования и сбору материала к работе.

Задание на ВКР с указанием срока выполнения выдается руководителем ВКР до начала преддипломной практики и утверждается заведующим выпускающей кафедрой.

Руководитель ВКР оказывает студенту помощь в разработке содержания темы на весь период выполнения ВКР, составлении календарного плана, рекомендует необходимую литературу, справочные материалы и другие источники по теме, проводит систематические консультации, проверяет выполнение работы по частям и в целом, составляет задания на преддипломную практику.

Консультанты (соруководители) проверяют соответствующую часть выполненной ВКР и ставят на ней свою подпись. При этом на титульном листе ВКР после данных о руководителе приводятся аналогичные данные о консультанте (соруководителе).

На заседаниях выпускающей кафедры не реже двух раз за период работы над выпускной квалификационной работой заслушиваются отчеты руководителей ВКР или студентов о степени готовности работы.

После окончания преддипломной практики проводится публичная предварительная защита работы, результаты которой фиксируются в протоколе заседания выпускающей кафедры.

Выполненная ВКР, подписанная студентом и консультантом, нормоконтролером представляется руководителю. После экспертизы ВКР (в том числе на объем заимствования в соответствии с Регламентом использования системы «Антиплагиат» • в СКФУ) руководитель подписывает ее и вместе со своим письменным отзывом о работе обучающегося в период подготовки выпускной квалификационной работы и с отзывом соруководителя (если предусмотрен) представляет работу заведующему кафедрой. В отзыве дается характеристика по всем разделам работы. В случае выполнения выпускной квалификационной работы несколькими обучающимися руководитель выпускной квалификационной работы представляет отзыв об их совместной работе в период подготовки выпускной квалификационной работы.

Заведующий кафедрой на основании этих материалов после заседания кафедры делает отметку на ВКР о допуске студента к защите. В случае, если студент не допускается к защите работы, этот вопрос рассматривается на заседании кафедры с участием руководителя. Протокол заседания кафедры о не допуске представляется в дирекцию факультета (филиала) и вместе со служебной запиской директора факультета (филиала) направляется на согласование к проректору по учебной работе.

Выпускные квалификационные работы по программам магистратуры подлежат рецензированию. Состав рецензентов из числа лиц, не являющихся работниками СКФУ, - специалистов научных и производственных учреждений по профилю специальности или других высших учебных заведений, утверждается распоряжением директора факультета (филиала) одновременно с темами выпускных квалификационных работ по представлению выпускающей кафедры. При подготовке распоряжения необходимо руководствоваться тем, что количество рецензируемых работ на одного рецензента - не более восьми.

ВКР, допущенная выпускающей кафедрой к защите, не позднее, чем за 10 дней календарных дней до защиты в государственной экзаменационной комиссии, направляется одному или нескольким рецензентам.

Если выпускная квалификационная работа имеет междисциплинарный характер, она направляется нескольким рецензентам. Рецензент проводит анализ выпускной квалификационной работы и представляет письменную рецензию на указанную работу (далее - рецензия). В рецензии необходимо отметить актуальность выбранной темы, степень ее обоснованности, целесообразность постановки задач исследования, полноту их реализации, аргументацию выводов, новизну, теоретическую и практическую значимость работы, дать общую оценку работы.

Выпускающая кафедра должна ознакомить обучающегося с отзывом и рецензией (рецензиями) не позднее, чем за 5 календарных дней до дня защиты выпускной квалификационной работы.

Выпускная квалификационная работа, отзыв и рецензия (рецензии) передаются в государственную экзаменационную комиссию не позднее чем за 2 календарных дня до дня защиты выпускной квалификационной работы.

Порядок проведения государственной итоговой аттестации выпускников определяется Положением о порядке проведения государственной итоговой аттестации по образовательным программам высшего образования – программам бакалавриата, программам специалитета и программам магистратуры в федеральном государственном автономном образовательном учреждении высшего образования «Северо-Кавказский федеральный университет».

8. Список рекомендуемой литературы, информационных источников

8.1 Основная литература

1. Алферов, А.П. Основы криптографии: Учебное пособие / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. – М.: Гелиос АРВ, 2019.
2. Бабенко, Л.К. Современные алгоритмы блочного шифрования и методы их анализа / Л.К. Бабенко, Е.А. Ищукова. – М.: Гелиос АРВ, 2018.
3. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам: Учебное пособие. М.: Горячая линия - Телеком, 2019. – 416 с.
4. Корнеев И.К. Защита информации в офисе: учеб. – М.: ТК Велби, Изд-во Проспект, 2018. – 336 с.
5. Корт С.С. Теоретические основы защиты информации: Учебное пособие. - М.: – Гелиос АРВ, 2018. – 240с.
6. Организация и современные методы защиты информации /Под общей редакцией Диева С.А., Шаваева А.Г./ - М.: Концерн «Банковский Деловой Центр», 2018. – 472с.
7. Петраков А.В., Дорошенко П.С., Савлуков Н.В. Охрана и защита современного предприятия. М.: Энергоатомиздат, 2019. – 568с
8. Правовое обеспечение информационной безопасности: учебник / [под общ.науч. ред. В. А. Минаева и др.]. – Изд. 2-е, расш. и доп. - Москва: Маросейка, 2018. - 368 с.
9. Соболев А.Н., Кириллов В.М. Физические основы технических средств обеспечения информационной безопасности. – М.: Гелиос АРВ, 2019. – 224 с.
10. Шевцов В.А., Куприянов А.И., Сахаров А.В. Основы защиты информации. – М.

Издательский дом «Академия», 2018. – 256 с.

8.2 Основная литература

5. Алферов, А.П. Основы криптографии: Учебное пособие / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. – М.: Гелиос АРВ, 2019.
6. Бабенко, Л.К. Современные алгоритмы блочного шифрования и методы их анализа / Л.К. Бабенко, Е.А. Ищукова. – М.: Гелиос АРВ, 2018.
7. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам: Учебное пособие. М.: Горячая линия - Телеком, 2019. – 416 с.
8. Корнеев И.К. Защита информации в офисе: учеб. – М.: ТК Велби, Изд-во Проспект, 2018. – 336 с.
9. Корт С.С. Теоретические основы защиты информации: Учебное пособие. - М.: – Гелиос АРВ, 2019. – 240с.
10. Организация и современные методы защиты информации /Под общей редакцией Диева С.А., Шаваева А.Г./ - М.: Концерн «Банковский Деловой Центр», 2006. – 472с.
11. Петраков А.В., Дорошенко П.С., Савлуков Н.В. Охрана и защита современного предприятия. М.: Энергоатомиздат, 2019. – 568с
12. Правовое обеспечение информационной безопасности: учебник / [под общ.науч. ред. В. А. Минаева и др.]. - Изд. 2-е, расш. и доп. - Москва: Маросейка, 2018. – 368 с.
13. Соболев А.Н., Кириллов В.М. Физические основы технических средств обеспечения информационной безопасности. – М.: Гелиос АРВ, 2018. – 224 с.
14. Шевцов В.А., Куприянов А.И., Сахаров А.В. Основы защиты информации. – М. Издательский дом «Академия», 2018. – 256 с.

8.3 Интернет-ресурсы

1. Сайт ФСТЭК России // Федеральная служба по техническому и экспортному контролю: [сайт]. — URL: <https://fstec.ru/> (дата обращения: 04.02.2025).
2. Сайт Роскомнадзора // Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций: [сайт]. — URL: <https://rkn.gov.ru/> (дата обращения: 04.02.2025).
3. Сайт ФСБ России // Федеральная служба безопасности Российской Федерации: [сайт]. — URL: <http://fsb.ru/> (дата обращения: 04.02.2025).
4. «Лань». Электронно-библиотечная система // Консорциум сетевых электронных библиотек ЭБС «Лань»: [сайт]. — URL: <https://e.lanbook.com/> (дата обращения: 04.02.2025).
5. Библиоклуб.РУ // ЭБС «Университетская библиотека ОНЛАЙН»: [сайт]. — URL: <https://www.biblioclub.ru/> (дата обращения: 04.02.2025).
6. Цифровой образовательный ресурс IPR SMART // ЭБС IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/> (дата обращения: 04.02.2025).
7. Znanium.com. // ЭБС Znanium: [сайт]. — URL: <https://znanium.com/> (дата обращения: 04.02.2025).
8. ЭБС «Юрайт». // Юрайт. Образовательная платформа: [сайт]. — URL: <http://www.biblio-online.ru> (дата обращения: 04.02.2025).
9. Поисковые интернет-системы Яндекс, Rambler, Google и др.

9. Описание показателей и критериев оценивания компетенций, а также шкал оценивания

9.1 Описание показателей

Уровни сформированности компетенции (ий), индикатора (ов)	Дескрипторы			
	Минимальный уровень не достигнут (Неудовлетворительно) 2 балла	Минимальный уровень (удовлетворительно) 3 балла	Средний уровень (хорошо) 4 балла	Высокий уровень (отлично) 5 баллов
ПК-1 Способен проводить исследования и анализ информационных процессов защиты информации в киберфизических системах				
Результаты прохождения практики: Индикаторы: ПК-1 ИД-1 классификация и систематизация информации по теме научного исследования, методы анализа и выбора решений по обеспечению требуемого уровня безопасности информационных процессов	на низком уровне: знает порядок подбора классификации и систематизации информации по теме научного исследования, методы анализа и выбора решений по обеспечению требуемого уровня безопасности информационных процессов с использованием современных достижений науки в области анализ информационных процессов, защиты информации в киберфизических системах,	в основном: порядок подбора классификации и систематизации информации по теме научного исследования, методы анализа и выбора решений по обеспечению требуемого уровня безопасности информационных процессов с использованием современных достижений науки в области анализ информационных процессов, защиты информации в киберфизических системах,	знает: порядок подбора классификации и систематизации информации по теме научного исследования, методы анализа и выбора решений по обеспечению требуемого уровня безопасности информационных процессов с использованием современных достижений науки в области анализ информационных процессов, защиты информации в киберфизических системах,	на высоком профессиональном уровне: порядок подбора классификации и систематизации информации по теме научного исследования, методы анализа и выбора решений по обеспечению требуемого уровня безопасности информационных процессов с использованием современных достижений науки в области анализ информационных процессов, защиты информации в киберфизических системах,
ПК-1 ИД-2 технологии поиска, изучения, обобщения и систематизации научной информации, методы анализа и обоснования выбора решений по обеспечению требуемого уровня безопасности информационных процессов защиты информации в киберфизических системах	на низком уровне: применяет технологии поиска, изучения, обобщения и систематизации научной информации, методы анализа и обоснования выбора решений по обеспечению требуемого уровня безопасности информационных процессов защиты информации в киберфизических системах	в основном: применяет технологии поиска, изучения, обобщения и систематизации научной информации, методы анализа и обоснования выбора решений по обеспечению требуемого уровня безопасности информационных процессов защиты информации в киберфизических системах	умеет: применять технологии поиска, изучения, обобщения и систематизации научной информации, методы анализа и обоснования выбора решений по обеспечению требуемого уровня безопасности информационных процессов защиты информации в киберфизических системах	на высоком профессиональном уровне: применяет технологии поиска, изучения, обобщения и систематизации научной информации, методы анализа и обоснования выбора решений по обеспечению требуемого уровня безопасности информационных процессов защиты информации в киберфизических системах

ПК-1 ИД-3 применения современных информационных технологий и программных средств, при решении задач профессиональной деятельности	на низком уровне: навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности	в основном: навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности	владеет: навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности	на высоком профессиональном уровне: навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности
ПК-2 Способен проектировать и реализовывать политику безопасности вычислительных сетей в киберфизических системах				
Результаты прохождения практики: Индикаторы: ПК-2 ИД-1 разрабатывает политику безопасности в киберфизических системах	на низком уровне знает состав, назначение и порядок разработки политики безопасности в киберфизических системах,	в основном знает состав, назначение и порядок разработки политики безопасности в киберфизических системах,	знает состав, назначение и порядок разработки политики безопасности в киберфизических системах,	на высоком профессиональном уровне знает состав, назначение и порядок разработки политики безопасности в киберфизических системах
ПК-2 ИД-2 проектирует политику безопасности вычислительных сетей в киберфизических системах	на низком уровне умеет применять современные информационные технологии, при проектировании политики безопасности вычислительных сетей в киберфизических системах	в основном умеет применять современные информационные технологии, при проектировании политики безопасности вычислительных сетей в киберфизических системах	умеет применять современные информационные технологии, при проектировании политики безопасности вычислительных сетей в киберфизических системах	на высоком профессиональном уровне умеет применять современные информационные технологии, при проектировании политики безопасности вычислительных сетей в киберфизических системах
ПК-2 ИД-3 реализует комплекс выбранных мер, при реализации политики безопасности вычислительных сетей в киберфизических системах	на низком уровне владеет навыками реализации комплекса выбранных мер, при реализации политики безопасности вычислительных сетей в киберфизических системах	в основном владеет навыками реализации комплекса выбранных мер, при реализации политики безопасности вычислительных сетей в киберфизических системах	владеет навыками реализации комплекса выбранных мер, при реализации политики безопасности вычислительных сетей в киберфизических системах	на высоком профессиональном уровне владеет навыками реализации комплекса выбранных мер, при реализации политики безопасности вычислительных сетей в киберфизических системах
ПК-3 Способен разрабатывать предложения по совершенствованию системы управления информационной безопасностью киберфизических систем				

ПК-3 ИД-1 порядок функционирования и алгоритм построения системы управления информационной безопасностью киберфизических систем	на низком уровне знает порядок функционирования системы управления информационной безопасностью киберфизических систем	в основном знает порядок функционирования системы управления информационной безопасностью киберфизических систем	знает порядок функционирования системы управления информационной безопасностью киберфизических систем	на высоком профессиональном уровне знает порядок функционирования системы управления информационной безопасностью киберфизических систем
ПК-3 ИД-2 анализ уязвимости и построение модели угроз для киберфизических систем	на низком уровне умеет строить модель угроз для киберфизических систем	в основном умеет строить модель угроз для киберфизических систем	умеет строить модель угроз для киберфизических систем	на высоком профессиональном уровне умеет строить модель угроз для киберфизических систем
ПК-3 ИД-3 выбора и реализации набора организационно-технических и криптографических мер в системе информационной безопасности киберфизических систем	на низком уровне владеет навыками реализации набора организационно-технических и криптографических мер в системе информационной безопасности киберфизических систем	в основном владеет навыками реализации набора организационно-технических и криптографических мер в системе информационной безопасности киберфизических систем	владеет навыками реализации набора организационно-технических и криптографических мер в системе информационной безопасности киберфизических систем	на высоком профессиональном уровне владеет навыками реализации набора организационно-технических и криптографических мер в системе информационной безопасности киберфизических систем
ПК-4 Способен оценивать уровень защищенности киберфизических систем и применять решения по обеспечению их информационной безопасности				
ПК- 4 ИД-1 оценка уровня защищённости киберфизических систем, анализ их структурно-функциональных характеристик	на низком уровне знает методики оценки уровня защищённости киберфизических систем, анализа их структурно-функциональных характеристик	в основном знает методики оценки уровня защищённости киберфизических систем, анализа их структурно-функциональных характеристик	Знает методики оценки уровня защищённости киберфизических систем, анализа их структурно-функциональных характеристик	на высоком профессиональном уровне знает методики оценки уровня защищённости киберфизических систем, анализа их структурно-функциональных характеристик
ПК- 4 ИД-2 определение уязвимости киберфизических систем	на низком уровне умеет определять уязвимости	в основном умеет определять уязвимости	Умеет определять уязвимости	на высоком профессиональном уровне умеет определять

	киберфизических систем	киберфизических систем	киберфизических систем	уязвимости киберфизических систем
ПК- 4 ИД-3 реализации организационно- технических мероприятий по обеспечению защиты киберфизических систем	на низком уровне владеет навыками реализации организационно- технических мероприятий по обеспечению защиты киберфизических систем	в основном владеет навыками реализации организационно- технических мероприятий по обеспечению защиты киберфизических систем	Владеет навыками реализации организационно- технических мероприятий по обеспечению защиты киберфизических систем	на высоком профессиональном уровне владеет навыками реализации организационно- технических мероприятий по обеспечению защиты киберфизических систем

9.2 Критерии оценивания компетенций на защите выпускной квалификационной работы

Оценка «отлично» выставляется обучающему, если студент на высоком уровне: знает порядок подбора классификации и систематизации информации по теме научного исследования, методы анализа и выбора решений по обеспечению требуемого уровня безопасности информационных процессов с использованием современных достижений науки в области анализ информационных процессов, защиты информации в киберфизических системах, умеет применять технологии поиска, изучения, обобщения и систематизации научной информации, методы анализа и обоснования выбора решений по обеспечению требуемого уровня безопасности информационных процессов защиты информации в киберфизических системах, владеет навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности, состав, назначение и порядок разработки политики безопасности в киберфизических системах, порядок определения уровня защищенности киберфизических систем, умеет применять современные информационные технологии, при проектировании политики безопасности вычислительных сетей в киберфизических системах, выбирать оптимальный набор организационных мер для повышения защищённости киберфизических систем, владеет навыками реализации комплекса выбранных мер, при реализации политики безопасности вычислительных сетей в киберфизических системах, навыками реализации организационно-технических мероприятий по обеспечению защиты киберфизических систем, состав системы управления информационной безопасностью киберфизических систем, порядок анализа структурно-функциональных характеристик киберфизических систем, умеет анализировать уязвимости киберфизических систем, выбирать оптимальный набор технических мер для повышения защищённости киберфизических систем, владеет навыками выбора набора организационно-технических и криптографических мер в системе информационной безопасности киберфизических систем, выбора организационно-технических мероприятий по обеспечению защиты киберфизических систем

Оценка «хорошо» выставляется студенту, если студент на хорошем уровне знает порядок подбора классификации и систематизации информации по теме научного исследования, методы анализа и выбора решений по обеспечению требуемого уровня безопасности информационных процессов с использованием современных достижений науки в области анализ информационных процессов, защиты информации в киберфизических системах, умеет применять технологии поиска, изучения, обобщения и систематизации научной информации, методы анализа и обоснования выбора решений по обеспечению требуемого уровня безопасности информационных процессов защиты информации в киберфизических системах, владеет навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности, состав, назначение и порядок разработки политики безопасности в киберфизических системах, порядок определения уровня защищенности киберфизических систем, умеет применять современные информационные технологии, при проектировании политики безопасности вычислительных сетей в киберфизических системах, выбирать оптимальный набор организационных мер для повышения защищённости киберфизических систем, владеет навыками реализации комплекса выбранных мер, при реализации политики безопасности вычислительных сетей в киберфизических системах,

навыками реализации организационно-технических мероприятий по обеспечению защиты киберфизических систем, состав системы управления информационной безопасностью киберфизических систем, порядок анализа структурно-функциональных характеристик киберфизических систем, умеет анализировать уязвимости киберфизических систем, выбирать оптимальный набор технических мер для повышения защищённости киберфизических систем, владеет навыками выбора набора организационно-технических и криптографических мер в системе информационной безопасности киберфизических систем, выбора организационно-технических мероприятий по обеспечению защиты киберфизических систем

Оценка «удовлетворительно» выставляется студенту, если студент на удовлетворительном уровне знает порядок подбора классификации и систематизации информации по теме научного исследования, методы анализа и выбора решений по обеспечению требуемого уровня безопасности информационных процессов с использованием современных достижений науки в области анализ информационных процессов, защиты информации в киберфизических системах, умеет применять технологии поиска, изучения, обобщения и систематизации научной информации, методы анализа и обоснования выбора решений по обеспечению требуемого уровня безопасности информационных процессов защиты информации в киберфизических системах, владеет навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности, состав, назначение и порядок разработки политики безопасности в киберфизических системах, порядок определения уровня защищённости киберфизических систем, умеет применять современные информационные технологии, при проектировании политики безопасности вычислительных сетей в киберфизических системах, выбирать оптимальный набор организационных мер для повышения защищённости киберфизических систем, владеет навыками реализации комплекса выбранных мер, при реализации политики безопасности вычислительных сетей в киберфизических системах, навыками реализации организационно-технических мероприятий по обеспечению защиты киберфизических систем, состав системы управления информационной безопасностью киберфизических систем, порядок анализа структурно-функциональных характеристик киберфизических систем, умеет анализировать уязвимости киберфизических систем, выбирать оптимальный набор технических мер для повышения защищённости киберфизических систем, владеет навыками выбора набора организационно-технических и криптографических мер в системе информационной безопасности киберфизических систем, выбора организационно-технических мероприятий по обеспечению защиты киберфизических систем

Оценка «неудовлетворительно» выставляется студенту, если студент на низком уровне знает порядок подбора классификации и систематизации информации по теме научного исследования, методы анализа и выбора решений по обеспечению требуемого уровня безопасности информационных процессов с использованием современных достижений науки в области анализ информационных процессов, защиты информации в киберфизических системах, умеет применять технологии поиска, изучения, обобщения и систематизации научной информации, методы анализа и обоснования выбора решений по обеспечению требуемого уровня безопасности информационных процессов защиты информации в киберфизических системах, владеет навыками применения современных информационных технологий и программных средств, в том числе отечественного

производства, при решении задач профессиональной деятельности, состав, назначение и порядок разработки политики безопасности в киберфизических системах, порядок определения уровня защищенности киберфизических систем, умеет применять современные информационные технологии, при проектировании политики безопасности вычислительных сетей в киберфизических системах, выбирать оптимальный набор организационных мер для повышения защищенности киберфизических систем, владеет навыками реализации комплекса выбранных мер, при реализации политики безопасности вычислительных сетей в киберфизических системах, навыками реализации организационно-технических мероприятий по обеспечению защиты киберфизических систем, состав системы управления информационной безопасностью киберфизических систем, порядок анализа структурно-функциональных характеристик киберфизических систем, умеет анализировать уязвимости киберфизических систем, выбирать оптимальный набор технических мер для повышения защищенности киберфизических систем, владеет навыками выбора набора организационно-технических и криптографических мер в системе информационной безопасности киберфизических систем, выбора организационно-технических мероприятий по обеспечению защиты киберфизических систем

9.3 Описание шкалы оценивания

Защита выпускной квалификационной работы оценивается по 5-балльной системе.

10. Приложения

ПРИЛОЖЕНИЕ А
(обязательное)

Заявка
на выполнение выпускной квалификационной работы

от «__» _____ 2026 года

Предприятие (организация): _____

(наименование организации)

просит организацию-исполнителя ФГАОУ ВО «Северо-Кавказский федеральный университет» кафедру организации и технологии защиты информации выполнить выпускную квалификационную работу на тему _____

Заказчик:

Исполнитель:

(подпись, расшифровка подписи)

(подпись, расшифровка подписи)

МП

МП

ПРИЛОЖЕНИЕ Б

(обязательное)

УТВЕРЖДАЮ

_____ 2026 г.

МП

АКТ

об использовании (внедрении) выводов и предложений автора выпускной квалификационной работы студента (ки) _____ в организации (на предприятии)

_____ (наименование организации (предприятия))

в лице _____

(должность и ФИО)

с одной стороны, и студента (ки) СКФУ _____

ФИО)

с другой стороны, составили настоящий акт об использовании (внедрении) результатов выпускной _____ квалификационной _____ работы _____ на тему _____

При внедрении предложений (использовании выводов) выпускной квалификационной работы достигнуты следующие основные результаты:

Представители организации:

Студент (ка):

(подпись, расшифровка подписи)

(подпись, расшифровка подписи)

(подпись, расшифровка подписи)

ПРИЛОЖЕНИЕ В

(обязательное)

Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования «СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Факультет математики и компьютерных наук имени профессора Н.И.Червякова
Кафедра организации и технологии защиты информации

Утверждена распоряжением по факультету
от « » 20 г. №

Выполнена по заявке организации
(предприятия)

Допущена к защите
« » июня 2026 г.

Зав. кафедрой организации и
технологии защиты информации
канд. техн. наук, доцент

В. И. Петренко

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

ОРГАНИЗАЦИЯ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В «СТАВРОПОЛЬПРОМСТРОЙБАНКЕ ОАО»

Рецензенты:

Петров Василий Евгеньевич

канд. техн. наук, доц., доцент кафедры

информационных систем и технологий

ФГБОУ ВО «Ставропольский

государственный аграрный университет

Выполнил (а):

Айриян Армен Артурович

студент (ка) 3 курса, группы ИНБ-м-оз-171

направления подготовки 10.04.01

«Информационная безопасность»

направленность (профиль) «Комплексная

защита объектов информатизации» очной

формы обучения

(подпись)

Нормоконтролер:

Иванов Иван Иванович

канд. техн. наук, доцент, доцент

кафедры организации и технологии

защиты информации

(подпись)

Руководитель:

Иванов Иван Иванович

канд. техн. наук, доцент, доцент

кафедры организации и технологии

защиты информации

(подпись)

Дата защиты «27» июня 2026 г.

Оценка

Ставрополь, 2026 г.

ПРИЛОЖЕНИЕ Г
(обязательное)

Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования «СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Факультет	математики и компьютерных наук имени профессора Н.И.Червякова
Кафедра	организации и технологии защиты информации
Направление	Информационная безопасность
Направленность (профиль)	Комплексная защита объектов информатизации

УТВЕРЖДАЮ

Зав. кафедрой организации и
технологии защиты информации
канд. техн. наук, доцент
В. И. Петренко

«13» апреля 2026 г.

ЗАДАНИЕ НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ РАБОТУ

Студент	Айриян Армен Артурович		группа	ИНБ-м-о -211
1. Тема	Организация системы защиты персональных данных в «Ставропольпромстройбанк ОАО»			
Утверждена распоряжением по факультету			№ 033-р/12. от «13» апреля 2026 г.	
2. Срок представления работы к защите			«20» июня 2023_ г.	
3. Исходные данные для выполнения работы			Работу выполнить в соответствии с требованиями ФЗ №152-ФЗ «О персональных данных» и стандартов Банка России	
4. Содержание бакалаврской работы:				
4.1 Анализ структуры, деятельности и организации защиты персональных данных в «Ставропольстройпромбанк ОАО».				
4.2 Организация системы защиты персональных данных в «Ставропольпромстройбанк ОАО».				
4.3 Оценка соответствия предложенных мер требованиям стандартов Банка России.				
4.4 Техничко-экономическое обоснование результатов работы				
Приложение				
Дата выдачи задания	«13» апреля 2026 г.			
Руководитель работы			И.И. Иванов	
	(подпись)		(инициалы, фамилия)	
Консультанты по разделам				
	(подпись)		(инициалы, фамилия)	
	(подпись)		(инициалы, фамилия)	
	(подпись)		(инициалы, фамилия)	
Задание к исполнению принял	«13» апреля 2026 г.		А.А. Айриян	
			подпись	

ПРИЛОЖЕНИЕ Д
(обязательное)
СОДЕРЖАНИЕ

Задание на выпускную квалификационную работу (бакалаврскую работу)

ВВЕДЕНИЕ **Error! Bookmark not defined.**

1 Проведение обследования ИС ФБУ «Ставропольский ЦСМ» по требованиям ЗИ и
определение этапов работы по разработке СЗИ в ИС организации **Error! Bookmark not defined.**

1.1 Анализ структуры и деятельности ФБУ «Ставропольский ЦСМ»

1.2 Анализ ИС ФБУ «Ставропольский ЦСМ»

1.3 Анализ требований нормативно-методических документов, регламентирующих
порядок разработки СЗИ в ГИС **Error! Bookmark not defined.**

1.4 Обоснование направлений исследований..... **Error! Bookmark not defined.**

1.5 Выводы по разделу..... **Error! Bookmark not defined.**

2 Разработка системы ЗИ в информационной системе ФБУ «Ставропольский ЦСМ»

2.1 Выбор мер ЗИ в ИС ФБУ «Ставропольский ЦСМ»..... **Error! Bookmark not defined.**

2.2 Выбор базового набора мер по ЗИ в ИС ФБУ «Ставропольский ЦСМ» **Error! Bookmark not defined.**

2.3 Адаптация базового набора мер по обеспечению безопасности информации в ИС ФБУ
«Ставропольский ЦСМ».....

2.4 Уточнение адаптированного набора мер по ЗИ в ИС ФБУ «Ставропольский ЦСМ»

2.4.1 Построение частной модели угроз для ИС ФБУ «Ставропольский ЦСМ».....

2.5 Выбор средств ЗИ в ИС ФБУ «Ставропольский ЦСМ».....

2.6 Выводы по разделу..... **Error! Bookmark not defined.**

3 Оценка эффективности разработанной СЗИ и технико-экономическое обоснование
результатов работы..... **Error! Bookmark not defined.**

3.1 Оценка эффективности разработанной СЗИ в ИС ФБУ «Ставропольский ЦСМ»

3.2 Техничко-экономическое обоснование результатов работы.....

3.3 Выводы по разделу..... **Error! Bookmark not defined.**

ЗАКЛЮЧЕНИЕ

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ..... **Error! Bookmark not defined.**

ПРИЛОЖЕНИЕ А (обязательное) Журнал учёта инцидентов

ПРИЛОЖЕНИЕ Ж

(обязательное)

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

Статья в периодических изданиях и сборниках статей:

1 Гуреев В.Н., Маэов НА Использование библиометрии для оценки значимости журналов в научных библиотечках (обзор)// Научно-техническая информация. Сер. 1. —2018. — № 2. —С. 8—19.

2 Колкова Н.И., Скипор И.Л. Термин системы предметной области «электронные информационные ресурсы»: взгляд с позиций теории и практики // Научн. и техн. б-ки. — 2016. — № 7. — С. 24—41.

Книги, монографии:

1 Земсхов А.И., Шрайберг Я.Л. Электронные библиотеки: учебник для вузов. — М.: Пиберея. 2013. — 351 с.

2 Костюк К.Н. Книга в новой медицинской среде. — М.: Директ-Медиа. 2015. —430 с.

Тезисы докладов, материалы конференций:

1 Пеготин Е.Ю. Организация метаданных в хранилище данных // Научный поиск. Технические науки: Материалы 3-й науч. конф. аспирантов и докторантов / огв. за вып. СД. Ваулин: Юж.-Урал. гос. ун-т. Т. 2. — Челябинск: Издательский центр ЮУрГУ. 2011. — С. 128—132.

2 Ангопольский А.Б. Система метаданных в электронных библиотеках II Библиотеки и ассоциации в меняющемся мире: Новые технологии и новые формы сотрудничества: Тр. 8-й Междунар. конф. «Крым-2001» / г. Судак, (июнь 2001 г.). — Т. 1. — М., 2001. — С. 287—298.

Электронные ресурсы:

1 Статистические показатели российского книгоиздания в 2006 г.: цифры и рейтинги (Электронный ресурс]. — 2006. — URL: http://pyrbookhambw.ru/stat_2006.htm (дата обращения 12.03.2009).

2 Прогноз научно-технологического развития Российской Федерации на период до 2030 года. — URL: <http://government.ru/media/fiies/41d4b737638891da21&4/pdf> (дата обращения 15.11.2016).

3 Web of Science. — URL: <http://apps.wbofknowledge.com/> (дата обращения 15.11.2016).

ПРИЛОЖЕНИЕ 3

(обязательное)

Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Факультет	математики и компьютерных наук имени профессора Н.И.Червякова
Кафедра	организации и технологии защиты информации
Направление	Информационная безопасность
Направленность (профиль)	Комплексная защита объектов информатизации

КАЛЕНДАРНЫЙ ПЛАН

Фамилия, имя, отчество Айриян Армен Артурович

Тема ВКР Организация системы защиты персональных данных в

«Ставропольпромстройбанке ОАО»

Руководитель Иванов И.И.

Консультанты:

№	Наименование этапов выпускной квалификационной работы	Срок выполнения работы	Примечание
1.	Анализ литературы по теме работы		
2.	Анализ нормативной базы, регламентирующей требования к организации работы по обеспечению защиты персональных данных в ИСПДн		
3.	Разработка методики выбора и реализации организационных и технических мер по обеспечению безопасности персональных данных, при их обработке в ИСПДн		
4.	Оценка эффективности системы защиты персональных данных, при их обработке в ИСПДн		
5.	Предварительная защита		
6.	Представление ВКР руководителю и нормоконтролёру		
7.	Представление ВКР заведующему кафедрой		
8.	Рецензирование		
9.	Представление ВКР в ГЭК		

Руководитель
Зав. кафедрой

И.И. Иванов
В.И. Петренко

«29» марта 2026 г.

ПРИЛОЖЕНИЕ И

(обязательное)

Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Факультет математики и компьютерных наук имени профессора Н.И.Червякова
Кафедра организации и технологии защиты информации

ОТЗЫВ РУКОВОДИТЕЛЯ

о работе в период подготовки выпускной квалификационной работы

студента Айрияна Армена Артуровича

направления подготовки 10.04.01. «Информационная безопасность»

направленности (профиля) Комплексная защита объектов информатизации

над выпускной квалификационной работой на тему «Организация системы защиты персональных данных в «Ставропольпромстройбанке ОАО»

Руководитель выпускной квалификационной работы Иванов Иван Иванович канд. техн. наук, доцент, доцент

1. Заключение о степени соответствия ВКР теме, утвержденной распоряжением декана факультета, и заданию на ВКР

2. Характеристика работы студента в период подготовки выпускной квалификационной работы

3. Оценка студента как специалиста:

4. Замечания руководителя:

5. Заключение и оценка ВКР (соответствует или не соответствует предъявляемым требованиям, заключение об уровне освоения компетенций, рекомендуемая оценка: отлично, хорошо, удовлетворительно):

6. Заключение о допуске к защите в государственной экзаменационной комиссии

«13» июня 2026 г. ...

.....
Подпись руководителя ВКР

ПРИЛОЖЕНИЕ К

(обязательное)

ЗАЯВЛЕНИЕ О САМОСТОЯТЕЛЬНОМ ХАРАКТЕРЕ ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ

Я, _____, студент _____ курса, направление подготовки «Информационная безопасность», профиль программы «Организация и технология защиты информации» заявляю, что в моей выпускной квалификационной работе на тему: «_____», представленной в государственную экзаменационную комиссию для публичной защиты (представления), не содержится элементов плагиата.

Все прямые заимствования из печатных и электронных источников, а также из защищенных ранее выпускных квалификационных работ /научных докладов кандидатских и докторских диссертаций имеют соответствующие ссылки.

Я ознакомлен(а) с действующим в Университете Регламентом использования системы «Антиплагиат» в федеральном государственном автономном образовательном учреждении высшего образования «Северо-Кавказский федеральный университет», согласно которому обнаружение плагиата является основанием для не допуска выпускной квалификационной работы к защите.

подпись

«__» _____ 20__ г.

ПРИЛОЖЕНИЕ Л

(обязательное)

ЖУРНАЛ УЧЕТА

проверки выпускных квалификационных работ / научных докладов в системе «Антиплагиат ВУЗ»

Направление подготовки «Информационная безопасность»

Направленность (профиль) программы аспирантуры /профиль/магистерская программа

Группа ИНБ-

№ п/п	Ф.И.О студента / аспиранта	Тема ВКР/научного доклада	Дата представления на проверку	Результат проверки: % оригинальности работы. Рекомендована к защите (представлению)/возвращена на проверку	Подпись студента /аспиранта ВКР	Дата представления на повторную проверку (при необходимости)	Результат повторной проверки: % оригинальности работы Рекомендована (не рекомендована) к защите (представлению)	Подпись студента / аспиранта
1.								
2.								
3.								
4.								
5.								
6.								
7.								
8.								
9.								

ПРИЛОЖЕНИЕ М

(обязательное)

Рецензия на выпускную квалификационную работу

Иванова Ивана Ивановича

выпускника ФГАОУ ВО «Северо-Кавказский федеральный университет»		
Направление подготовки 10.04.01 «Информационная безопасность»		
Группа ИНБ-м-о-211 группы	Форма обучения	Очно
1. Тема	Разработка методики выбора и реализации организационных и технических мер по обеспечению безопасности персональных данных, при их обработке в информационных системах персональных данных	
2. Дата представления выпускной квалификационной работы на рецензию:	27 ноября 2023 г.	
3. Дата возвращения выпускной квалификационной работы:	28 ноября 2023 г.	
4. Актуальность темы:	тема актуальна, т.к. в современных условиях хозяйствования с развитием средств вычислительной техники увеличивается количество угроз для информационных систем персональных данных (ИСПДн)	
5. Заключение о степени соответствия темы и содержания ВКР заданию:	выпускная квалификационная работа Иванова И.И. полностью соответствует теме и заданию.	
6. Уровень и качество теоретической и научно-исследовательской проработки проблемы:	исследования, проведённые в работе, носят выраженный научно-исследовательский характер, работа выполнена в строгом соответствии с требованиями нормативных документов регламентирующих порядок защиты информации в информационных системах персональных данных.	
7. Полнота и проблемность, вносимых предложений:	тема работы раскрыта полностью, проблемы, рассматриваемые в работе актуальны.	
8. Объем экспериментальных исследований и возможность внедрения в производство:	объём экспериментальных исследований достаточный, построенный на экспертных оценках, результаты работы могут быть полезны, при организации работ по модернизации ИСПДн.	
9. Характеристика каждого раздела работы и степень использования выпускником последних достижений науки и техники:	структурно работа состоит из введения, трёх разделов и заключения. Во введении обосновывается необходимость повышения качества защиты информации в ИСПДн. В первом разделе, проведён анализ структуры и деятельности ЗАО «Кристалл», разработана частная модель угроз, на основании которой выявлены актуальные угрозы для ИСПДн предприятия, определены направления исследования. Во втором разделе, с учётом требований нормативных документов по защите персональных данных, с учётом особенностей информационной системы предприятия, разработанной частной модели угроз, разработан комплекс мер по защите ИСПДн предприятия. В третьем разделе проведена оценка эффективности модернизированной системы защиты ИСПДн и технико-экономическое обоснование возможности реализации рекомендованных мер. В заключении анализируется проделанная работа, оцениваются результаты Исследования.	
10. Оценка качества пояснительной записки и графической части:	пояснительная записка	

выполнена с учётом требований нормативных документов к такого рода работам.

11. Достоинства ВКР: работа носит ярко выраженную практическую направленность, т. к. все исследования проведены в соответствии с требованиями нормативных документов и

заканчиваются конкретными рекомендациями по модернизации ИСПДн предприятия.

12. Основные недостатки работы: в качестве недостатка можно отметить несколько упрощённый подход к оценке затрат на реализацию предложенных мер по защите ИСПДн предприятия.

13. Заключение и оценка ВКР: выпускная квалификационная работа Бисюкова В.М. полностью соответствует требованиям, предъявляемым к такого рода работам, и заслуживает оценки «отлично».

14. Заключение (рекомендация) о присвоении квалификации: Бисюков В.М. достоин присвоения квалификации «магистр» по направлению «Информационная безопасность».

15. Должность, фамилия, имя, отчество, ученое звание, степень рецензента: директор ООО «СГУ Инфоком» Демурчев Никита Георгиевич канд. техн. наук, доцент

Подпись рецензента _____

«15» июня 2026 г.

М.П.

Памятка рецензенту: При рецензировании ВКР просим учесть, что рецензия должна содержать заключения:

- об актуальности темы,
- о степени обоснованности темы и соответствия выполненной выпускной квалификационной работы заданию,
- целесообразности постановки задач исследования,
- уровне и качестве теоретической и научно-исследовательской проработки проблемы,
- полноте и проблемности вносимых предложений по рассматриваемой проблеме,
- объеме экспериментальных исследований и возможности внедрения в производство,
- характеристике каждого раздела работы (проекта) и степени использования выпускником последних достижений науки и техники,
- оценке качества пояснительной записки и графической части,
- перечне положительных качеств ВКР и основных недостатках, критические замечания, теоретической и практической значимости работы,
- о степени самостоятельности разработки,
- об уровне освоения компетенций и готовности выпускника к практической деятельности,
- дать общую оценку выпускной квалификационной работы.

Перечень тем выпускных квалификационных работ (по видам

№ п/п	Наименование темы выпускной квалификационной работы
1.	Разработка технического регламента применения электронной подписи в корпоративной информационной системе организации
2.	Разработка рекомендаций по защите информации на значимом объекте критической информационной инфраструктуры
3.	Разработка рекомендаций по защите информации в локальной сети коммерческой организации
4.	Разработка рекомендаций по построению системы защиты информации на значимых объектах критической информационной инфраструктуры
5.	Разработка предложений по повышению защищённости информации в телефонных линиях предприятия
6.	Разработка рекомендаций по мониторингу сетевых ресурсов в беспроводной сети организации
7.	Разработка рекомендаций по обеспечению комплексной защиты информации в коммерческом банке
8.	Разработка предложений по защите коммерческой тайны организации
9.	Разработка рекомендаций по защите корпоративной сети организации на основе анализа трафика с помощью технологий искусственного интеллекта
10.	Разработка теоретических и практических рекомендаций по реализации системы контроля и управления доступом к информационной системе предприятия
11.	Разработка предложений по аттестации информационной системы персональных данных предприятия
12.	Разработка регламента защиты информационных ресурсов организации на основе биометрической аутентификации
13.	Разработка предложений по защите web-сервера под управлением операционной системы Ubuntu от DDoS- атак
14.	Разработка рекомендаций по защите автоматизированной системы управления технологическим процессом организации от угроз информационной безопасности
15.	Разработка модели угроз информационной безопасности организации (на материалах ООО «Вера- СК» г. Ставрополь)
16.	Разработка рекомендаций по построению системы защиты информации в автоматизированных системах управления технологическими процессами
17.	Разработка рекомендаций по введению режима коммерческой тайны в ПАО «Сигнал»
18.	Разработка рекомендаций по построению системы доступа к коммерческой тайне организации
19.	Разработка рекомендаций по построению системы защиты информации в государственной информационной системе
20.	Разработка рекомендаций по администрированию смарт беспроводной среды кофейни на базе прогрессивного протокола IEEE 802.11 ax
21.	Разработка частного технического задания на создание системы защиты персональных данных в информационной системе персональных данных АО «Электроавтоматика»
22.	Разработка рекомендаций по обеспечению защиты информации в удостоверяющем центре
23.	Разработка рекомендаций по созданию интегрированной системы управления доступом к защищаемым информационным ресурсам организации
24.	Разработка модели угроз для информационной системы персональных данных организации

25.	Разработка рекомендаций по реализации системы обнаружения и предотвращения атак на WEB-приложения
26.	Разработка рекомендаций по защите информации в учреждении здравоохранения
27.	Разработка рекомендаций по защите информации в государственном казённом учреждении Ставропольского края "Краевой центр информационных технологий"
28.	Разработка регламента пропускного режима организации на основе процедур идентификации и аутентификации
29.	Разработка рекомендаций по построению системы защиты персональных данных в информационной системе персональных данных предприятия
30.	Разработка рекомендаций по построению информационной системы контроля безопасности бизнеса от персонала (внутреннего нарушителя)
31.	Разработка регламента проведения внутреннего аудита информационной безопасности организации
32.	Разработка теоретических и практических рекомендаций по реализации системы информационной защиты для локальной сети предприятия
33.	Разработка рекомендаций по защите беспроводной сети предприятия
34.	Разработка частной модели угроз безопасности персональных данных при их обработке в информационной системе организации
35.	Разработка рекомендаций по организационной защите физическим лицом своих персональных данных в условиях "транзитного мира" и эффективного перехода к цифровой эпохе
36.	Разработка комплекса мероприятий по обеспечению защиты информации государственной информационной системы паспортно-визовых документов нового поколения
37.	Разработка рекомендаций по защите информационновычислительной сети организации с использованием решений ViPNet
38.	Разработка рекомендаций по организации защиты персональных данных в Межрегиональном филиале ФКУ «ЦОКР» в г. Ставрополе
39.	Разработка рекомендаций по защите персональных данных в информационных системах Некоммерческой организации микрокредитной компании «Фонд микрофинансирования субъектов малого и среднего предпринимательства в Ставропольском крае»
40.	Разработка предложений по маскированию информации в компьютерных сетях
41.	Разработка рекомендаций по совершенствованию метода биометрической аутентификации по клавиатурному почерку

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

Декан факультета математики и
компьютерных наук имени
профессора Н.И. Червякова
_____ Т. А. Грובה

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

Направление подготовки	<u>10.04.01 Информационная безопасность</u>
Направленность (профиль)/специализация	<u>Информационная безопасность киберфизических систем</u>
Год начала обучения	<u>2026</u>
Форма обучения	<u>очная</u>
Реализуется в семестре	<u>4</u>

СОГЛАСОВАНО:

Представитель работодателя
Директор ООО «Инфоком С»
_____ Н.Г. Демурчев

РАЗРАБОТАНО:

Доцент кафедры организации и
технологии защиты информации
Бисюков Виктор Михайлович

1. Предисловие

1. Фонд оценочных средств предназначен для проведения государственной итоговой аттестации магистров направления 10.04.01 «Информационная безопасность».

2. Фонд оценочных средств итоговой аттестации разработан на основе программы Государственной итоговой аттестации в соответствии с образовательной программой по направлению подготовки 10.04.01 «Информационная безопасность», утвержденной на заседании Учёного совета СКФУ протокол № ____ от « » _____ 2026_ г.

3. Разработчики: Петренко В.И., зав. кафедрой организации и технологии защиты информации и Бисюков В.М., доцент кафедры организации и технологии защиты информации.

4. ФОС рассмотрен и утвержден на заседании кафедры «Организация и технология защиты информации», Протокол №__ от _____ 2026_ года.

5. Проведена экспертиза ФОС. Члены экспертной группы, проводившие внутреннюю экспертизу:

Председатель _____ В.И. Петренко, зав. кафедрой
_____ И.В. Мандрица, профессор
_____ Т.В. Минкина, доцент.
_____ Н.Г. Демурчев, директор ООО «Инфоком С»

Экспертное заключение рекомендовано к апробации в учебном процессе

«__» _____ В.И. Петренко

«__» _____ Н.Г. Демурчев

6. Срок действия ФОС: на период действия ОП.

1. Перечень компетенций, которыми должны овладеть обучающиеся в результате освоения образовательной программы

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
ОПК-1	Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание
ОПК-2	Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности
ОПК-3	Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности
ОПК-4	Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок
ОПК-5	Способен проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи
ПК-1	Способен проводить исследования и анализ информационных процессов защиты информации в киберфизических системах
ПК-2	Способен проектировать и реализовывать политику безопасности вычислительных сетей в киберфизических системах
ПК-3	Способен разрабатывать предложения по совершенствованию системы управления информационной безопасностью киберфизических систем
ПК-4	Способен оценивать уровень защищенности киберфизических систем и применять решения по обеспечению их информационной безопасности

2. Паспорт фонда оценочных средств для проведения государственной итоговой аттестации

№ п/п	Модуль, раздел	Контролируемые компетенции (или их части)	ФОС	
			Вид оценочного средства	Количество вариантов заданий
1	Государственный междисциплинарный экзамен			
1.1	1.1 Теоретические основы компьютерной безопасности	УК-1, УК- 2, УК- 3, УК-4, УК- 5, УК- 6	Вопросы по темам/разделам дисциплины	32
1.2	1.2 Технологии обеспечения информационной безопасности	УК- 5, УК- 6, ОПК-1, ОПК-2, ОПК-3, ОПК-4, ОПК-5	Вопросы по темам/разделам дисциплины	35
1.3	1.3 Защищённые информационные системы	УК-1, УК- 2, УК- 3, УК-4, УК- 5, УК- 6, ОПК-1, ОПК-2, ОПК-3, ОПК-4, ОПК-5	Вопросы по темам/разделам дисциплины	35
1.4	1.4 Основы научных исследований	ОПК-1, ОПК-2, ОПК-3, ОПК-4, ОПК-5	Вопросы по темам/разделам дисциплины	27
2	Выпускная квалификационная работа			
2.1	Раздел 1	ПК-1, ПК-2, ПК-3, ПК-4	Темы докладов, сообщений	18
2.2	Раздел 2	ПК ПК-1, ПК-2, ПК-3, ПК-4	Темы докладов, сообщений	18
2.3	Раздел 3	ПК-1, ПК-2, ПК-3, ПК-4	Темы докладов, сообщений	18

Составитель _____ В.М. Бисюков
(подпись)

« ____ » _____ 2026 г.

3. Описание показателей и критериев оценивания компетенций, а также шкал оценивания

3.1 Описание показателей

Уровни сформированности компетенции (ий), индикатора (ов)	Дескрипторы			
	Минимальный уровень не достигнут (неудовлетворительно) 2 балла	Минимальный уровень (удовлетворительно) 3 балла	Средний уровень (хорошо) 4 балла	Высокий уровень (отлично) 5 баллов
УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий				
Результаты обучения: <i>Индикатор:</i> ИД-1 УК-1 выделяет проблемную ситуацию, осуществляет ее критический анализ и диагностику на основе системного подхода	с грубыми ошибками подбирает технологии поиска и критического анализа информации, использует методы системного подхода для решения поставленных задач с помощью цифровых и информационных технологий, организует личное цифровое пространство,	в основном подбирает технологии поиска и критического анализа информации, использует методы системного подхода для решения поставленных задач с помощью цифровых и информационных технологий, организует личное цифровое пространство,	подбирает технологии поиска и критического анализа информации, использует методы системного подхода для решения поставленных задач с помощью цифровых и информационных технологий, организует личное цифровое пространство,	в полном объеме подбирает технологии поиска и критического анализа информации, использует методы системного подхода для решения поставленных задач с помощью цифровых и информационных технологий, организует личное цифровое пространство,
ИД-2 УК-1 осуществляет поиск, сбор и обработку информации для определения альтернативных вариантов стратегических действий в проблемной ситуации	с грубыми ошибками определяет и оценивает риски возможных вариантов решений проблемной ситуации, выбирает оптимальный вариант её решения.	в основном осуществляет поиск, отбор и систематизацию информации для определения альтернативных вариантов стратегических решений в проблемной ситуации	осуществляет поиск, отбор и систематизацию информации для определения альтернативных вариантов стратегических решений в проблемной ситуации	в полном объеме осуществляет поиск, анализ, оценку, отбор и систематизацию информации для определения альтернативных вариантов стратегических решений в проблемной ситуации
ИД-3 УК-1 определяет и оценивает риски возможных вариантов решений проблемной ситуации, вырабатывает стратегию действий по решению проблемной ситуации	на низком уровне выделяет и оценивает риски возможных вариантов решений проблемной ситуации, вырабатывает стратегию действий по решению проблемной ситуации	в основном выделяет и оценивает риски возможных вариантов решений проблемной ситуации, вырабатывает стратегию действий по решению проблемной ситуации	выделяет и оценивает риски возможных вариантов решений проблемной ситуации, вырабатывает стратегию действий по решению проблемной ситуации	в полном объеме выделяет и оценивает риски возможных вариантов решений проблемной ситуации, вырабатывает стратегию действий по решению проблемной ситуации
УК -2 Способен управлять проектом на всех этапах его жизненного цикла				
ИД-1 УК-2 формулирует	на низком уровне	в основном осуществляет	осуществляет учёт	в полном объеме

цель проекта, определяют совокупность взаимосвязанных задач, обеспечивающих ее достижение на всех этапах его жизненного цикла	осуществляет учёт требований законодательных и правовых актах РФ, регулирующих правовые отношения в сфере информационной безопасности и защиты государственной тайны, применяет цифровые технологии для решения проектных задач, выбирая оптимальный способ их решения, исходя из действующих правовых норм и имеющихся ресурсов и ограничений	учёт требований законодательных и правовых актах РФ, регулирующих правовые отношения в сфере информационной безопасности и защиты государственной тайны, применяет цифровые технологии для решения проектных задач, выбирая оптимальный способ их решения, исходя из действующих правовых норм и имеющихся ресурсов и ограничений	требований законодательных и правовых актах РФ, регулирующих правовые отношения в сфере информационной безопасности и защиты государственной тайны, применяет цифровые технологии для решения проектных задач, выбирая оптимальный способ их решения, исходя из действующих правовых норм и имеющихся ресурсов и ограничений	осуществляет учёт требований законодательных и правовых актах РФ, регулирующих правовые отношения в сфере информационной безопасности и защиты государственной тайны, применяет цифровые технологии для решения проектных задач, выбирая оптимальный способ их решения, исходя из действующих правовых норм и имеющихся ресурсов и ограничений
ИД-2 УК-2 разрабатывает план действий по управлению проектом на всех этапах его жизненного цикла	с грубыми ошибками обеспечивает выполнение проекта в соответствии с установленными целями, сроками и затратами, исходя из действующих правовых норм, имеющихся ресурсов и ограничений, в том числе с использованием цифровых инструментов	в основном обеспечивает выполнение проекта в соответствии с установленными целями, сроками и затратами, исходя из действующих правовых норм, имеющихся ресурсов и ограничений, в том числе с использованием цифровых инструментов	обеспечивает выполнение проекта в соответствии с установленными целями, сроками и затратами, исходя из действующих правовых норм, имеющихся ресурсов и ограничений, в том числе с использованием цифровых инструментов	в полном объёме обеспечивает выполнение проекта в соответствии с установленными целями, сроками и затратами, исходя из действующих правовых норм, имеющихся ресурсов и ограничений, в том числе с использованием цифровых инструментов
ИД-3 УК-2 обеспечивает контроль выполнения и оценивает эффективность реализации проекта на всех этапах его жизненного цикла	с грубыми ошибками проводит контроль выполнения и оценивает эффективность реализации проекта на всех этапах его жизненного цикла	в основном проводит контроль выполнения и оценивает эффективность реализации проекта на всех этапах его жизненного цикла	проводит контроль выполнения и оценивает эффективность реализации проекта на всех этапах его жизненного цикла	в полном объёме проводит контроль выполнения и оценивает эффективность реализации проекта на всех этапах его жизненного цикла
УК -3 Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели				
ИД-1 УК-3 разрабатывает цель и задачи командной	ан низким уровне осознает свою роль в системе	в основном осознает свою роль в системе	осознает свою роль в системе межличностного	в полном объёме осознает свою роль в системе

работы, используя инклюзивный подход, эффективную коммуникацию, методы командообразования и командного взаимодействия при совместной работе	межличностного взаимодействия, анализирует стратегии поведения в группе, и особенности поведения разных групп людей, с которыми работает (взаимодействует),	межличностного взаимодействия, анализирует стратегии поведения в группе, и особенности поведения разных групп людей, с которыми работает (взаимодействует),	взаимодействия, анализирует стратегии поведения в группе, и особенности поведения разных групп людей, с которыми работает (взаимодействует),	межличностного взаимодействия, анализирует стратегии поведения в группе, и особенности поведения разных групп людей, с которыми работает (взаимодействует),
ИД-2 УК-3 организует работу команды для получения оптимальных результатов совместной работы, с учетом индивидуальных возможностей её членов, использования методологии достижения успеха, методов, информационных технологий и технологий фортсайта	с грубыми ошибками определяет статус и роль членов группы в системе межличностных отношений и учитывает на практике эти показатели, при этом меняет методы командной работы, обеспечивает выполнение поставленных задач на основе мониторинга командной работы и своевременного реагирования на существенные отклонения.	в основном определяет статус и роль членов группы в системе межличностных отношений и учитывает на практике эти показатели, при этом меняет методы командной работы, обеспечивает выполнение поставленных задач на основе мониторинга командной работы и своевременного реагирования на существенные отклонения.	определяет статус и роль членов группы в системе межличностных отношений и учитывает на практике эти показатели, при этом меняет методы командной работы, обеспечивает выполнение поставленных задач на основе мониторинга командной работы и своевременного реагирования на существенные отклонения.	в полном объеме определяет статус и роль членов группы в системе межличностных отношений и учитывает на практике эти показатели, при этом меняет методы командной работы, обеспечивает выполнение поставленных задач на основе мониторинга командной работы и своевременного реагирования на существенные отклонения.
ИД-3 УК-3 руководит выполнением поставленных задач на основе мониторинга командной работы и своевременного реагирования на существенные отклонения	с грубыми ошибками руководит выполнением поставленных задач на основе мониторинга командной работы и своевременного реагирования на существенные отклонения	в основном руководит выполнением поставленных задач на основе мониторинга командной работы и своевременного реагирования на существенные отклонения	руководит выполнением поставленных задач на основе мониторинга командной работы и своевременного реагирования на существенные отклонения	в полном объеме руководит выполнением поставленных задач на основе мониторинга командной работы и своевременного реагирования на существенные отклонения
УК-4 Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия				
ИД-1 УК-4 выбирает приемлемый стиль делового общения на государственном(-ых) и иностранном(-ых) языках, вербальные и невербальные	на низком уровне руководствуется правилами деловой коммуникации в устной и письменной формах на государственном языке РФ и иностранном(ых) языке(ах),	в основном руководствуется правилами деловой коммуникации в устной и письменной формах на государственном языке РФ и иностранном(ых) языке(ах),	руководствуется правилами деловой коммуникации в устной и письменной формах на государственном языке РФ и иностранном(ых) языке(ах),	в полном объеме руководствуется правилами деловой коммуникации в устной и письменной формах на государственном языке РФ и иностранном(ых) языке(ах),

средства взаимодействия с партнерами в устной и письменной формах	пользуется современными средствами деловой коммуникации на основе информационных технологий, осуществляет поиск и анализ требуемой информации в профессиональном взаимодействии, проводит оценку эффективности применяемых информационных технологий	пользуется современными средствами деловой коммуникации на основе информационных технологий, осуществляет поиск и анализ требуемой информации в профессиональном взаимодействии, проводит оценку эффективности применяемых информационных технологий	пользуется современными средствами деловой коммуникации на основе информационных технологий, осуществляет поиск и анализ требуемой информации в профессиональном взаимодействии, проводит оценку эффективности применяемых информационных технологий	пользуется современными средствами деловой коммуникации на основе информационных технологий, осуществляет поиск и анализ требуемой информации в профессиональном взаимодействии, проводит оценку эффективности применяемых информационных технологий
ИД-2 УК-4 применяет современные коммуникационные технологии для повышения эффективности профессионального взаимодействия, поиска необходимой информации в процессе решения стандартных коммуникативных задач на государственном(-ых) и иностранном(-ых) языках	допускает грубые ошибки при решении профессиональных задач с использованием современных коммуникационных технологий, при поиске необходимой информации в процессе решения стандартных коммуникативных задач на государственном(-ых) и иностранном(-ых) языках	в основном решает профессиональные задачи с использованием современных коммуникационных технологий, проводит поиск необходимой информации в процессе решения стандартных коммуникативных задач на государственном(-ых) и иностранном(-ых) языках	решает профессиональные задачи с использованием современных коммуникационных технологий, проводит поиск необходимой информации в процессе решения стандартных коммуникативных задач на государственном(-ых) и иностранном(-ых) языках	в полном объеме решает профессиональные задачи с использованием современных коммуникационных технологий, проводит поиск необходимой информации в процессе решения стандартных коммуникативных задач на государственном(-ых) и иностранном(-ых) языках
ИД-3 УК-4 оценивает эффективность применяемых коммуникативных технологий в профессиональном взаимодействии на государственном (-ых) и иностранном (-ых) языках, производит выбор	на низком уровне проводит оценку эффективности применяемых коммуникативных технологий в профессиональном взаимодействии на государственном (-ых) и иностранном (-ых) языках, производит выбор оптимальных решений	в основном проводит оценку эффективности применяемых коммуникативных технологий в профессиональном взаимодействии на государственном (-ых) и иностранном (-ых) языках, производит выбор	проводит оценку эффективности применяемых коммуникативных технологий в профессиональном взаимодействии на государственном (-ых) и иностранном (-ых) языках, производит выбор	в полном объеме проводит оценку эффективности применяемых коммуникативных технологий в профессиональном взаимодействии на государственном (-ых) и иностранном (-ых) языках, производит выбор

оптимальных		оптимальных решений	оптимальных решений	оптимальных решений
УК-5 Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия				
ИД-1 УК-5 - выявляет, сопоставляет и анализирует информацию о культурных особенностях и традициях различных социальных групп, для выбора стратегии взаимодействия с их носителями	на низком уровне учитывает культурные особенности и традиции различных социальных групп, этносов и конфессий, анализируя социальные ситуации взаимодействия	в основном учитывает культурные особенности и традиции различных социальных групп, этносов и конфессий, анализируя социальные ситуации взаимодействия	учитывает культурные особенности и традиции различных социальных групп, этносов и конфессий, анализируя социальные ситуации взаимодействия	в полном объеме учитывает культурные особенности и традиции различных социальных групп, этносов и конфессий, анализируя социальные ситуации взаимодействия
ИД-2 УК-5 демонстрирует уважительное отношение к историческому наследию и социокультурным традициям различных социальных групп, опирающееся на знание этапов исторического развития России (включая основные события, основных исторических деятелей) в контексте мировой истории и ряда культурных традиций мира (в зависимости от среды и задач образования), включая мировые религии, философские и этические учения	на низком уровне проявляет уважение к историческому наследию и социокультурным традициям различных социальных групп, опирающееся на знание этапов исторического развития России (включая основные события, основных исторических деятелей) в контексте мировой истории и ряда культурных традиций мира (в зависимости от среды и задач образования), включая мировые религии, философские и этические учения	в основном проявляет уважение к историческому наследию и социокультурным традициям различных социальных групп, опирающееся на знание этапов исторического развития России (включая основные события, основных исторических деятелей) в контексте мировой истории и ряда культурных традиций мира (в зависимости от среды и задач образования), включая мировые религии, философские и этические учения	проявляет уважение к историческому наследию и социокультурным традициям различных социальных групп, опирающееся на знание этапов исторического развития России (включая основные события, основных исторических деятелей) в контексте мировой истории и ряда культурных традиций мира (в зависимости от среды и задач образования), включая мировые религии, философские и этические учения	в полном объеме проявляет уважение к историческому наследию и социокультурным традициям различных социальных групп, опирающееся на знание этапов исторического развития России (включая основные события, основных исторических деятелей) в контексте мировой истории и ряда культурных традиций мира (в зависимости от среды и задач образования), включая мировые религии, философские и этические учения
ИД-3 УК-5 - выбирает способы конструктивного взаимодействия с людьми с учетом их социокультурных особенностей в целях успешного выполнения	на низком уровне выбирает формы, методы, приемы взаимодействия с различными социальными группами, учитывает культурные и религиозные традиции, при	в основном выбирает формы, методы, приемы взаимодействия с различными социальными группами, учитывает культурные и религиозные	выбирает формы, методы, приемы взаимодействия с различными социальными группами, учитывает культурные и религиозные традиции, при личном и	в полном объеме выбирает формы, методы, приемы взаимодействия с различными социальными группами, учитывает культурные и религиозные

профессиональных задач и усиления социальной интеграции	личном и массовом общении, определяет приемы конструктивного взаимодействия в ситуации общения	традиции, при личном и массовом общении, определяет приемы конструктивного взаимодействия в ситуации общения	массовом общении, определяет приемы конструктивного взаимодействия в ситуации общения	традиции, при личном и массовом общении, определяет приемы конструктивного взаимодействия в ситуации общения
УК – 6 Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни				
ИД-1 УК-6 устанавливает личные и профессиональные цели в соответствии с уровнем своих ресурсов и приоритетов действий, для успешного развития в избранной сфере профессиональной деятельности	допускает грубые ошибки, при постановке целей в своей профессиональной деятельности и решении профессиональных задач с учётом своих ресурсных возможностей и приоритетов, выборе эффективной стратегии и тактики личностного и профессионального развития, пользуется методикой оценки применяемых методов решения поставленных задач в сфере своей профессиональной деятельности	в основном ставит цели в своей профессиональной деятельности и решает профессиональные задачи с учётом своих ресурсных возможностей и приоритетов, выбирает эффективные стратегии и тактики личностного и профессионального развития, пользуется методикой оценки эффективности применяемых методов решения поставленных задач в сфере своей профессиональной деятельности	ставит цели в своей профессиональной деятельности и решает профессиональные задачи с учётом своих ресурсных возможностей и приоритетов, выбирает эффективные стратегии и тактики личностного и профессионального развития, пользуется методикой оценки эффективности применяемых методов решения поставленных задач в сфере своей профессиональной деятельности	в полном объёме ставит цели в своей профессиональной деятельности и решает профессиональные задачи с учётом своих ресурсных возможностей и приоритетов, выбирает эффективные стратегии и тактики личностного и профессионального развития, пользуется методикой оценки эффективности применяемых методов решения поставленных задач в сфере своей профессиональной деятельности
ИД-2 УК-6 реализует и корректирует стратегию своего личностного и профессионального развития с учетом условий, средств, личностных возможностей, этапов карьерного роста, временной перспективы развития деятельности и	с грубыми ошибками оценивает эффективность использования времени и других ресурсов при решении поставленных задач в избранной сфере профессиональной деятельности	в основном оценивает эффективность использования времени и других ресурсов при решении поставленных задач в избранной сфере профессиональной деятельности	оценивает эффективность использования времени и других ресурсов при решении поставленных задач в избранной сфере профессиональной деятельности	в полном объёме оценивает эффективность использования времени и других ресурсов при решении поставленных задач в избранной сфере профессиональной деятельности

требований рынка труда				
ИД-3 УК-6 критически оценивает эффективность использования своего времени и других ресурсов при решении задач, поставленных в избранной сфере профессиональной деятельности	с грубыми ошибками проводит критическую оценку эффективности использования своего времени и других ресурсов, при решении задач, поставленных в избранной сфере профессиональной деятельности	в основном проводит критическую оценку эффективности использования своего времени и других ресурсов, при решении задач, поставленных в избранной сфере профессиональной деятельности	проводит критическую оценку эффективности использования своего времени и других ресурсов, при решении задач, поставленных в избранной сфере профессиональной деятельности	в полном объеме проводит критическую оценку эффективности использования своего времени и других ресурсов, при решении задач, поставленных в избранной сфере профессиональной деятельности
ОПК – 1 Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание				
ИД-1 ОПК-1 проектирует информационные системы с учетом различных технологий обеспечения информационной безопасности	допускает грубые ошибки при решении задач моделирования и проектирования автоматизированных информационных систем и систем обеспечения информационной безопасности, разработке и обосновании критериев оценки эффективности проектируемой системы обеспечения информационной безопасности	в основном применяет методы решения задач моделирования и проектирования автоматизированных информационных систем и систем обеспечения информационной безопасности, разрабатывает и обосновывает критерии оценки эффективности проектируемой системы обеспечения информационной безопасности	применяет методы решения задач моделирования и проектирования автоматизированных информационных систем и систем обеспечения информационной безопасности, разрабатывает и обосновывает критерии оценки эффективности проектируемой системы обеспечения информационной безопасности	в полном объеме применяет методы решения задач моделирования и проектирования автоматизированных информационных систем и систем обеспечения информационной безопасности, разрабатывает и обосновывает критерии оценки эффективности проектируемой системы обеспечения информационной безопасности
ИД-2 ОПК-1 формирует актуальную модель угроз для автоматизированных информационных систем и учитывает её положения при формировании требований технического задания на проектируемую систему	с грубыми ошибками разрабатывает актуальную модель угроз для автоматизированных информационных систем и учитывает её положения при формировании требований технического задания на проектируемую систему	в основном разрабатывает актуальную модель угроз для автоматизированных информационных систем и учитывает её положения при формировании требований технического задания на проектируемую систему	разрабатывает актуальную модель угроз для автоматизированных информационных систем и учитывает её положения при формировании требований технического задания на проектируемую систему	в полном объеме разрабатывает актуальную модель угроз для автоматизированных информационных систем и учитывает её положения при формировании требований технического задания на проектируемую систему

обеспечения информационной безопасности	проектируемую систему обеспечения информационной безопасности	обеспечения информационной безопасности	систему обеспечения информационной безопасности	проектируемую систему обеспечения информационной безопасности
ИД-3 ОПК-1 разрабатывает и обосновывает критерии оценки эффективности проектируемой системы обеспечения информационной безопасности, оценивает эффективность решений и анализирует показатели деятельности	с грубыми ошибками проводит разработку и обосновывает критерии оценки эффективности проектируемой системы обеспечения информационной безопасности, оценивает эффективность решений и анализирует показатели деятельности	в основном проводит разработку и обосновывает критерии оценки эффективности проектируемой системы обеспечения информационной безопасности, оценивает эффективность решений и анализирует показатели деятельности	проводит разработку и обосновывает критерии оценки эффективности проектируемой системы обеспечения информационной безопасности, оценивает эффективность решений и анализирует показатели деятельности	в полном объеме проводит разработку и обосновывает критерии оценки эффективности проектируемой системы обеспечения информационной безопасности, оценивает эффективность решений и анализирует показатели деятельности
ОПК – 2 Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности				
ИД-1 ОПК-2 использует методы концептуального проектирования технологий обеспечения информационной безопасности	допускает грубые ошибки при определении направления развития и проблем компьютерного моделирования сложных систем, разработке и исследовании системы защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасности	в основном определяет направления развития и проблем компьютерного моделирования сложных систем, разработке и исследовании системы защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасности	определяет направления развития и проблем компьютерного моделирования сложных систем, разработке и исследовании системы защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасности	в полном объеме определяет направления развития и проблем компьютерного моделирования сложных систем, разработке и исследовании системы защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасности
ИД-2 ОПК-2 выбирает и обосновывает преимущества методов решения задач для защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью	на низком уровне реализовывает типовые задачи средствами автоматизированного и ручного функционального тестирования	в основном реализовывает типовые задачи средствами автоматизированного и ручного функционального тестирования	реализовывает типовые задачи средствами автоматизированного и ручного функционального тестирования	в полном объеме реализовывает типовые задачи средствами автоматизированного и ручного функционального тестирования

ИД-3 ОПК-2 решает типовые задачи разработки и исследования систем защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью	на низком уровне учитывает направления развития технологий проектирования информационных, автоматизированных и автоматических систем, управляет коллективом исполнителей и принимает управленческие решения,	в основном учитывает направления развития технологий проектирования информационных, автоматизированных и автоматических систем, управляет коллективом исполнителей и принимает управленческие решения,	учитывает направления развития технологий проектирования информационных, автоматизированных и автоматических систем, управляет коллективом исполнителей и принимает управленческие решения,	в полном объеме учитывает направления развития технологий проектирования информационных, автоматизированных и автоматических систем, управляет коллективом исполнителей и принимает управленческие решения,
ОПК – 3 Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности				
ИД-1 ОПК-3 разрабатывает технические задания на создание подсистем обеспечения информационной безопасности	допускает грубые ошибки при соблюдении правил построения оптимальной политики безопасности в соответствии с требованиями уровня безопасности, определении стоимости и сроков реализации проекта, выполнении работ с нормативными правовыми актами в области информационной безопасности с технической и эксплуатационной документацией, при оценке различных инструментов в области проектирования и управления информационной безопасности	в основном соблюдает правила построения оптимальной политики безопасности в соответствии с требованиями уровня безопасности, определяет стоимость и сроки реализации проекта, работает с нормативными правовыми актами в области информационной безопасности с технической и эксплуатационной документацией, оценивает различные инструменты в области проектирования и управления информационной безопасности	соблюдает правила построения оптимальной политики безопасности в соответствии с требованиями уровня безопасности, определяет стоимость и сроки реализации проекта, работает с нормативными правовыми актами в области информационной безопасности с технической и эксплуатационной документацией, оценивает различные инструменты в области проектирования и управления информационной безопасности	в полном объеме соблюдает правила построения оптимальной политики безопасности в соответствии с требованиями уровня безопасности, определяет стоимость и сроки реализации проекта, работает с нормативными правовыми актами в области информационной безопасности с технической и эксплуатационной документацией, оценивает различные инструменты в области проектирования и управления информационной безопасности
ИД-2 ОПК-3 разрабатывает проекты организационно-распорядительной документации по обеспечению информационной	допускает грубые ошибки при учёте требований отечественных и зарубежных стандартов в области сертификации и аттестации объектов информатизации,	в основном соблюдает основы отечественных и зарубежных стандартов в области сертификации и аттестации объектов информатизации, учитывает	соблюдает основы отечественных и зарубежных стандартов в области сертификации и аттестации объектов информатизации, учитывает	в полном объеме соблюдает основы отечественных и зарубежных стандартов в области сертификации и аттестации объектов информатизации, учитывает

безопасности	определении основных угроз безопасности информации и моделей нарушителя в информационных системах, разработке политик безопасности различных уровней, расчёте и разработке положения о применимости механизмов контроля в контексте управления рисками информационной безопасности	основные угрозы безопасности информации и модели нарушителя в информационных системах, разрабатывает политики безопасности различных уровней, рассчитывает и разрабатывает положения о применимости механизмов контроля в контексте управления рисками информационной безопасности	основные угрозы безопасности информации и модели нарушителя в информационных системах, разрабатывает политики безопасности различных уровней, рассчитывает и разрабатывает положения о применимости механизмов контроля в контексте управления рисками информационной безопасности	основные угрозы безопасности информации и модели нарушителя в информационных системах, разрабатывает политики безопасности различных уровней, рассчитывает и разрабатывает положения о применимости механизмов контроля в контексте управления рисками информационной безопасности
ИД-3 ОПК-3 проводит технико-экономическое обоснование проектных решений в области построения систем обеспечения информационной безопасности	допускает грубые ошибки при соблюдении правил построения оптимальной политики безопасности в соответствии с требованиями уровня безопасности, определении стоимости и сроков реализации проекта, выполнении работ с нормативными правовыми актами в области информационной безопасности с технической и эксплуатационной документацией, при оценке различных инструментов в области проектирования и управления информационной безопасности	в основном соблюдает правила построения оптимальной политики безопасности в соответствии с требованиями уровня безопасности, определяет стоимость и сроки реализации проекта, работает с нормативными правовыми актами в области информационной безопасности с технической и эксплуатационной документацией, оценивает различные инструменты в области проектирования и управления информационной безопасности	соблюдает правила построения оптимальной политики безопасности в соответствии с требованиями уровня безопасности, определяет стоимость и сроки реализации проекта, работает с нормативными правовыми актами в области информационной безопасности с технической и эксплуатационной документацией, оценивает различные инструменты в области проектирования и управления информационной безопасности	в полном объёме соблюдает правила построения оптимальной политики безопасности в соответствии с требованиями уровня безопасности, определяет стоимость и сроки реализации проекта, работает с нормативными правовыми актами в области информационной безопасности с технической и эксплуатационной документацией, оценивает различные инструменты в области проектирования и управления информационной безопасности
ОПК-4 Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок				
ИД-1 ОПК-4 осуществляет сбор и обработку	с грубыми ошибками формулирует научную	в основном формулирует научную проблему,	формулирует научную проблему, анализирует	в полном объёме формулирует научную

информации в глобальной компьютерной сети, проводит анализ научно-технической информации по теме исследования	проблему, анализирует гипотезы, проводит выбор предмета, объекта, целей, задач исследования, создаёт эскизный, технический, рабочий проект, применяет технологии поиска, изучения, обобщения и систематизации научной информации,	анализирует гипотезы, проводит выбор предмета, объекта, целей, задач исследования, создаёт эскизный, технический, рабочий проект, применяет технологии поиска, изучения, обобщения и систематизации научной информации	гипотезы, проводит выбор предмета, объекта, целей, задач исследования, создаёт эскизный, технический, рабочий проект, применяет технологии поиска, изучения, обобщения и систематизации научной информации	проблему, анализирует гипотезы, проводит выбор предмета, объекта, целей, задач исследования, создаёт эскизный, технический, рабочий проект, применяет технологии поиска, изучения, обобщения и систематизации научной информации
ИД-2 ОПК-4 разрабатывает пошаговый план и программу научной деятельности, проводит предпроектные исследования	с грубыми ошибками определяет комплекс мер для обеспечения безопасности информационных систем, составляет аналитические обзоры по вопросам обеспечения информационной безопасности систем, использует методы и средства анализа защищенности информационных систем, программные и аппаратные средства персонального компьютера для поиска и обработки информации	в основном определяет комплекс мер для обеспечения безопасности информационных систем, составляет аналитические обзоры по вопросам обеспечения информационной безопасности систем, использует методы и средства анализа защищенности информационных систем, программные и аппаратные средства персонального компьютера для поиска и обработки информации	определяет комплекс мер для обеспечения безопасности информационных систем, составляет аналитические обзоры по вопросам обеспечения информационной безопасности систем, использует методы и средства анализа защищенности информационных систем, программные и аппаратные средства персонального компьютера для поиска и обработки информации	в полном объёме определяет комплекс мер для обеспечения безопасности информационных систем, составляет аналитические обзоры по вопросам обеспечения информационной безопасности систем, использует методы и средства анализа защищенности информационных систем, программные и аппаратные средства персонального компьютера для поиска и обработки информации
ИД-3 ОПК-4 применяет методику создания технического задания и технического проекта при организации НИОКР	с грубыми ошибками формулирует научную проблему, анализирует гипотезы, применяет методику создания технического задания и технического проекта при организации НИОКР	в основном формулирует научную проблему, анализирует гипотезы, применяет методику создания технического задания и технического проекта при организации НИОКР	формулирует научную проблему, анализирует гипотезы, применяет методику создания технического задания и технического проекта при организации НИОКР	в полном объёме формулирует научную проблему, анализирует гипотезы, применяет методику создания технического задания и технического проекта при организации НИОКР

ОПК-5 Способен проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи.				
ИД-1 ОПК-5 применяет методы научных исследований в научной деятельности, в частности, при написании магистерской диссертации и научных статей	с грубыми ошибками определяет порядок организации процесса исследования, методы построения оптимальных планов для научных экспериментов, оформляет научные публикации в соответствии с шаблоном IEEE, требованиями научных конференций	в основном определяет порядок организации процесса исследования, методы построения оптимальных планов для научных экспериментов, оформляет научные публикации в соответствии с шаблоном IEEE, требованиями научных конференций	определяет порядок организации процесса исследования, методы построения оптимальных планов для научных экспериментов, оформляет научные публикации в соответствии с шаблоном IEEE, требованиями научных конференций	в полном объеме определяет порядок организации процесса исследования, методы построения оптимальных планов для научных экспериментов, оформляет научные публикации в соответствии с шаблоном IEEE, требованиями научных конференций
ИД-2 ОПК-5 оформляет научно-технические отчеты и обзоры по результатам проведенных экспериментальных исследований	с грубыми ошибками разрабатывает техническую документацию в соответствии с требованиями Единой системы конструкторской документации и Единой системы программной документации, анализирует получаемые результаты и формулирует выводы	в основном разрабатывает техническую документацию в соответствии с требованиями Единой системы конструкторской документации и Единой системы программной документации, анализирует получаемые результаты и формулирует выводы	разрабатывает техническую документацию в соответствии с требованиями Единой системы конструкторской документации и Единой системы программной документации, анализирует получаемые результаты и формулирует выводы	в полном объеме разрабатывает техническую документацию в соответствии с требованиями Единой системы конструкторской документации и Единой системы программной документации, анализирует получаемые результаты и формулирует выводы
ИД-3 ОПК-5 готовит научные доклады и статьи по результатам выполненных исследований	с грубыми ошибками выбирает и обосновывает критерии оценки защищенности открытых информационных систем, готовит научные доклады и статьи	в основном выбирает и обосновывает критерии оценки защищенности открытых информационных систем, готовит научные доклады и статьи	выбирает и обосновывает критерии оценки защищенности открытых информационных систем, готовит научные доклады и статьи	в полном объеме выбирает и обосновывает критерии оценки защищенности открытых информационных систем, готовит научные доклады и статьи
ПК-1 Способен проводить исследования и анализ информационных процессов защиты информации в киберфизических системах				
Результаты прохождения практики: Индикаторы: ПК-1 ИД-1 классификация и	на низком уровне: знает порядок подбора классификации и систематизации информации	в основном: порядок подбора классификации и систематизации информации по теме научного	знает: порядок подбора классификации и систематизации информации по теме	на высоком профессиональном уровне: порядок подбора классификации и

				задач профессиональной деятельности
ПК-2 Способен проектировать и реализовывать политику безопасности вычислительных сетей в киберфизических системах				
Результаты прохождения практики: Индикаторы: ПК-2 ИД-1 разрабатывает политику безопасности в киберфизических системах	на низком уровне знает состав, назначение и порядок разработки политики безопасности в киберфизических системах,	в основном знает состав, назначение и порядок разработки политики безопасности в киберфизических системах,	знает состав, назначение и порядок разработки политики безопасности в киберфизических системах,	на высоком профессиональном уровне знает состав, назначение и порядок разработки политики безопасности в киберфизических системах
ПК-2 ИД-2 проектирует политику безопасности вычислительных сетей в киберфизических системах	на низком уровне умеет применять современные информационные технологии, при проектировании политики безопасности вычислительных сетей в киберфизических системах	в основном умеет применять современные информационные технологии, при проектировании политики безопасности вычислительных сетей в киберфизических системах	умеет применять современные информационные технологии, при проектировании политики безопасности вычислительных сетей в киберфизических системах	на высоком профессиональном уровне умеет применять современные информационные технологии, при проектировании политики безопасности вычислительных сетей в киберфизических системах
ПК-2 ИД-3 реализует комплекс выбранных мер, при реализации политики безопасности вычислительных сетей в киберфизических системах	на низком уровне владеет навыками реализации комплекса выбранных мер, при реализации политики безопасности вычислительных сетей в киберфизических системах	в основном владеет навыками реализации комплекса выбранных мер, при реализации политики безопасности вычислительных сетей в киберфизических системах	владеет навыками реализации комплекса выбранных мер, при реализации политики безопасности вычислительных сетей в киберфизических системах	на высоком профессиональном уровне владеет навыками реализации комплекса выбранных мер, при реализации политики безопасности вычислительных сетей в киберфизических системах
ПК-3 Способен разрабатывать предложения по совершенствованию системы управления информационной безопасностью киберфизических систем				
ПК-3 ИД-1 порядок функционирования и алгоритм построения системы управления информационной	на низком уровне знает порядок функционирования системы управления информационной безопасностью	в основном знает порядок функционирования системы управления информационной безопасностью	знает порядок функционирования системы управления информационной безопасностью	на высоком профессиональном уровне знает порядок функционирования системы управления

безопасностью киберфизических систем	киберфизических систем	киберфизических систем	киберфизических систем	информационной безопасностью киберфизических систем
ПК-3 ИД-2 анализ уязвимости и построение модели угроз для киберфизических систем	на низком уровне умеет строить модель угроз для киберфизических систем	в основном умеет строить модель угроз для киберфизических систем	умеет строить модель угроз для киберфизических систем	на высоком профессиональном уровне умеет строить модель угроз для киберфизических систем
ПК-3 ИД-3 выбора и реализации набора организационно- технических и криптографических мер в системе информационной безопасности киберфизических систем	на низком уровне владеет навыками реализации набора организационно- технических и криптографических мер в системе информационной безопасности киберфизических систем	в основном владеет навыками реализации набора организационно- технических и криптографических мер в системе информационной безопасности киберфизических систем	владеет навыками реализации набора организационно- технических и криптографических мер в системе информационной безопасности киберфизических систем	на высоком профессиональном уровне владеет навыками реализации набора организационно- технических и криптографических мер в системе информационной безопасности киберфизических систем
ПК-4 Способен оценивать уровень защищенности киберфизических систем и применять решения по обеспечению их информационной безопасности				
ПК- 4 ИД-1 оценка уровня защищённости киберфизических систем, анализ их структурно- функциональных характеристик	на низком уровне знает методики оценки уровня защищённости киберфизических систем, анализа их структурно- функциональных характеристик	в основном знает методики оценки уровня защищённости киберфизических систем, анализа их структурно- функциональных характеристик	Знает методики оценки уровня защищённости киберфизических систем, анализа их структурно- функциональных характеристик	на высоком профессиональном уровне знает методики оценки уровня защищённости киберфизических систем, анализа их структурно- функциональных характеристик
ПК- 4 ИД-2 определение уязвимости киберфизических систем	на низком уровне умеет определять уязвимости киберфизических систем	в основном умеет определять уязвимости киберфизических систем	Умеет определять уязвимости киберфизических систем	на высоком профессиональном уровне умеет определять уязвимости киберфизических систем

ПК- 4 ИД-3 реализации организационно-технических мероприятий по обеспечению защиты киберфизических систем	на низком уровне владеет навыками реализации организационно-технических мероприятий по обеспечению защиты киберфизических систем	в основном владеет навыками реализации организационно-технических мероприятий по обеспечению защиты киберфизических систем	Владеет навыками реализации организационно-технических мероприятий по обеспечению защиты киберфизических систем	на высоком профессиональном уровне владеет навыками реализации организационно-технических мероприятий по обеспечению защиты киберфизических систем
---	--	--	---	--

3.2 Критерии оценивания компетенций на государственном экзамене

Оценка «отлично» выставляется обучающему, если студент на высоком уровне знает технологии поиска и критического анализа информации, использует методы системного подхода для решения поставленных задач с помощью цифровых и информационных технологий, организует личное цифровое пространство, осуществляет поиск, отбор и систематизацию информации для определения альтернативных вариантов стратегических решений в проблемной ситуации, выделяет и оценивает риски возможных вариантов решений проблемной ситуации, вырабатывает стратегию действий по решению проблемной ситуации, осуществляет учёт требований законодательных и правовых актов РФ, регулирующих правовые отношения в сфере информационной безопасности и защиты государственной тайны, применяет цифровые технологии для решения проектных задач, выбирая оптимальный способ их решения, исходя из действующих правовых норм и имеющихся ресурсов и ограничений, обеспечивает выполнение проекта в соответствии с установленными целями, сроками и затратами, исходя из действующих правовых норм, имеющихся ресурсов и ограничений, в том числе с использованием цифровых инструментов, проводит контроль выполнения и оценивает эффективность реализации проекта на всех этапах его жизненного цикла, осознает свою роль в системе межличностного взаимодействия, анализирует стратегии поведения в группе, и особенности поведения разных групп людей, с которыми работает (взаимодействует), определяет статус и роль членов группы в системе межличностных отношений и учитывает на практике эти показатели, применяет методы командной работы, обеспечивает выполнение поставленных задач на основе мониторинга командной работы и своевременного реагирования на существенные отклонения, руководит выполнением поставленных задач на основе мониторинга командной работы и своевременного реагирования на существенные отклонения, руководствуется правилами деловой коммуникации в устной и письменной формах на государственном языке РФ и иностранном(ых) языке(ах), пользуется современными средствами деловой коммуникации на основе информационных технологий, осуществляет поиск и анализ требуемой информации в профессиональном взаимодействии, проводит оценку эффективности применяемых информационных технологий, решает профессиональные задачи с использованием современных коммуникационных технологий, проводит поиск необходимой информации в процессе решения стандартных коммуникативных задач на государственном(-ых) и иностранном(-ых) языках, проводит оценку эффективности применяемых коммуникативных технологий в профессиональном взаимодействии на государственном (-ых) и иностранном (-ых) языках, производит выбор оптимальных решений, учитывает культурные особенности и традиции различных социальных групп, этносов и конфессий, анализируя социальные ситуации взаимодействия, проявляет уважение к историческому наследию и социокультурным традициям различных социальных групп, опирающееся на знание этапов исторического развития России (включая основные события, основных исторических деятелей) в контексте мировой истории и ряда культурных традиций мира (в зависимости от среды и задач образования), включая мировые религии, философские и этические учения, выбирает формы, методы, приемы взаимодействия с различными социальными группами, учитывает культурные и религиозные традиции, при личном и массовом общении, определяет приемы конструктивного взаимодействия в ситуации общения, ставит цели в своей профессиональной деятельности и решает профессиональные задачи с учётом своих ресурсных возможностей и приоритетов, выбирает эффективные стратегии и тактики личностного и профессионального развития, пользуется методикой оценки эффективности применяемых методов решения поставленных задач в сфере своей профессиональной деятельности, оценивает эффективность использования времени и других ресурсов при решении поставленных задач в избранной сфере профессиональной деятельности, проводит критическую оценку эффективности использования своего времени и других ресурсов, при решении задач, поставленных в избранной сфере профессиональной деятельности, применяет методы решения задач моделирования и

проектирования автоматизированных информационных систем и систем обеспечения информационной безопасности, разрабатывает и обосновывает критерии оценки эффективности проектируемой системы обеспечения информационной безопасности, разрабатывает актуальную модель угроз для автоматизированных информационных систем и учитывает её положения при формировании требований технического задания на проектируемую систему обеспечения информационной безопасности, проводит разработку и обосновывает критерии оценки эффективности проектируемой системы обеспечения информационной безопасности, оценивает эффективность решений и анализирует показатели деятельности, определяет направления развития и проблем компьютерного моделирования сложных систем, разработке и исследовании системы защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасности, реализовывает типовые задачи средствами автоматизированного и ручного функционального тестирования, учитывает направления развития технологий проектирования информационных, автоматизированных и автоматических систем, управляет коллективом исполнителей и принимает управленческие решения, соблюдает правила построения оптимальной политики безопасности в соответствии с требованиями уровня безопасности, определяет стоимость и сроки реализации проекта, работает с нормативными правовыми актами в области информационной безопасности с технической и эксплуатационной документацией, оценивает различные инструменты в области проектирования и управления информационной безопасности, соблюдает основы отечественных и зарубежных стандартов в области сертификации и аттестации объектов информатизации, учитывает основные угрозы безопасности информации и модели нарушителя в информационных системах, разрабатывает политики безопасности различных уровней, рассчитывает и разрабатывает положения о применимости механизмов контроля в контексте управления рисками информационной безопасности, соблюдает правила построения оптимальной политики безопасности в соответствии с требованиями уровня безопасности, определяет стоимость и сроки реализации проекта, работает с нормативными правовыми актами в области информационной безопасности с технической и эксплуатационной документацией, оценивает различные инструменты в области проектирования и управления информационной безопасности, соблюдает основы отечественных и зарубежных стандартов в области сертификации и аттестации объектов информатизации, учитывает основные угрозы безопасности информации и модели нарушителя в информационных системах, разрабатывает политики безопасности различных уровней, рассчитывает и разрабатывает положения о применимости механизмов контроля в контексте управления рисками информационной безопасности, формулирует научную проблему, анализирует гипотезы, проводит выбор предмета, объекта, целей, задач исследования, создаёт эскизный, технический, рабочий проект, применяет технологии поиска, изучения, обобщения и систематизации научной информации, определяет комплекс мер для обеспечения безопасности информационных систем, составляет аналитические обзоры по вопросам обеспечения информационной безопасности систем, использует методы и средства анализа защищенности информационных систем, программные и аппаратные средства персонального компьютера для поиска и обработки информации, формулирует научную проблему, анализирует гипотезы, применяет методику создания технического задания и технического проекта при организации НИОКР, определяет порядок организации процесса исследования, методы построения оптимальных планов для научных экспериментов, оформляет научные публикации в соответствие с шаблоном IEEE, требованиями научных конференций, разрабатывает техническую документацию в соответствии с требованиями Единой системы конструкторской документации и Единой системы программной документации, анализирует получаемые результаты и формулирует выводы, выбирает и обосновывает критерии оценки защищенности открытых информационных систем, готовит научные доклады и статьи, порядок подбора классификации и систематизации информации по теме научного исследования, методы анализа и выбора решений по обеспечению требуемого уровня безопасности информационных процессов с использованием современных достижений науки в области анализ информационных процессов, защиты

информации в киберфизических системах, умеет применять технологии поиска, изучения, обобщения и систематизации научной информации, методы анализа и обоснования выбора решений по обеспечению требуемого уровня безопасности информационных процессов защиты информации в киберфизических системах, владеет навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности, состав, назначение и порядок разработки политики безопасности в киберфизических системах, порядок определения уровня защищенности киберфизических систем, умеет применять современные информационные технологии, при проектировании политики безопасности вычислительных сетей в киберфизических системах, выбирать оптимальный набор организационных мер для повышения защищенности киберфизических систем, владеет навыками реализации комплекса выбранных мер, при реализации политики безопасности вычислительных сетей в киберфизических системах, навыками реализации организационно-технических мероприятий по обеспечению защиты киберфизических систем, состав системы управления информационной безопасностью киберфизических систем, порядок анализа структурно-функциональных характеристик киберфизических систем, умеет анализировать уязвимости киберфизических систем, выбирать оптимальный набор технических мер для повышения защищенности киберфизических систем, владеет навыками выбора набора организационно-технических и криптографических мер в системе информационной безопасности киберфизических систем, выбора организационно-технических мероприятий по обеспечению защиты киберфизических систем

Оценка «хорошо» выставляется студенту, если студент на хорошем уровне знает технологии поиска и критического анализа информации, использует методы системного подхода для решения поставленных задач с помощью цифровых и информационных технологий, организует личное цифровое пространство, осуществляет поиск, отбор и систематизацию информации для определения альтернативных вариантов стратегических решений в проблемной ситуации, выделяет и оценивает риски возможных вариантов решений проблемной ситуации, вырабатывает стратегию действий по решению проблемной ситуации, осуществляет учёт требований законодательных и правовых актов РФ, регулирующих правовые отношения в сфере информационной безопасности и защиты государственной тайны, применяет цифровые технологии для решения проектных задач, выбирая оптимальный способ их решения, исходя из действующих правовых норм и имеющихся ресурсов и ограничений, обеспечивает выполнение проекта в соответствии с установленными целями, сроками и затратами, исходя из действующих правовых норм, имеющихся ресурсов и ограничений, в том числе с использованием цифровых инструментов, проводит контроль выполнения и оценивает эффективность реализации проекта на всех этапах его жизненного цикла, осознает свою роль в системе межличностного взаимодействия, анализирует стратегии поведения в группе, и особенности поведения разных групп людей, с которыми работает (взаимодействует), определяет статус и роль членов группы в системе межличностных отношений и учитывает на практике эти показатели, применяет методы командной работы, обеспечивает выполнение поставленных задач на основе мониторинга командной работы и своевременного реагирования на существенные отклонения, руководит выполнением поставленных задач на основе мониторинга командной работы и своевременного реагирования на существенные отклонения, руководствуется правилами деловой коммуникации в устной и письменной формах на государственном языке РФ и иностранном(ых) языке(ах), пользуется современными средствами деловой коммуникации на основе информационных технологий, осуществляет поиск и анализ требуемой информации в профессиональном взаимодействии, проводит оценку эффективности применяемых информационных технологий, решает профессиональные задачи с использованием современных коммуникационных технологий, проводит поиск необходимой информации в процессе решения стандартных коммуникативных задач на государственном(-ых) и иностранном(-ых) языках, проводит оценку эффективности применяемых коммуникативных технологий в профессиональном взаимодействии на государственном (-ых) и

иностранном (-ых) языках, производит выбор оптимальных решений, учитывает культурные особенности и традиции различных социальных групп, этносов и конфессий, анализируя социальные ситуации взаимодействия, проявляет уважение к историческому наследию и социокультурным традициям различных социальных групп, опирающееся на знание этапов исторического развития России (включая основные события, основных исторических деятелей) в контексте мировой истории и ряда культурных традиций мира (в зависимости от среды и задач образования), включая мировые религии, философские и этические учения, выбирает формы, методы, приемы взаимодействия с различными социальными группами, учитывает культурные и религиозные традиции, при личном и массовом общении, определяет приемы конструктивного взаимодействия в ситуации общения, ставит цели в своей профессиональной деятельности и решает профессиональные задачи с учётом своих ресурсных возможностей и приоритетов, выбирает эффективные стратегии и тактики личностного и профессионального развития, пользуется методикой оценки эффективности применяемых методов решения поставленных задач в сфере своей профессиональной деятельности, оценивает эффективность использования времени и других ресурсов при решении поставленных задач в избранной сфере профессиональной деятельности, проводит критическую оценку эффективности использования своего времени и других ресурсов, при решении задач, поставленных в избранной сфере профессиональной деятельности, применяет методы решения задач моделирования и проектирования автоматизированных информационных систем и систем обеспечения информационной безопасности, разрабатывает и обосновывает критерии оценки эффективности проектируемой системы обеспечения информационной безопасности, разрабатывает актуальную модель угроз для автоматизированных информационных систем и учитывает её положения при формировании требований технического задания на проектируемую систему обеспечения информационной безопасности, проводит разработку и обосновывает критерии оценки эффективности проектируемой системы обеспечения информационной безопасности, оценивает эффективность решений и анализирует показатели деятельности, определяет направления развития и проблем компьютерного моделирования сложных систем, разработке и исследовании системы защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасности, реализовывает типовые задачи средствами автоматизированного и ручного функционального тестирования, учитывает направления развития технологий проектирования информационных, автоматизированных и автоматических систем, управляет коллективом исполнителей и принимает управленческие решения, соблюдает правила построения оптимальной политики безопасности в соответствии с требованиями уровня безопасности, определяет стоимость и сроки реализации проекта, работает с нормативными правовыми актами в области информационной безопасности с технической и эксплуатационной документацией, оценивает различные инструменты в области проектирования и управления информационной безопасности, соблюдает основы отечественных и зарубежных стандартов в области сертификации и аттестации объектов информатизации, учитывает основные угрозы безопасности информации и модели нарушителя в информационных системах, разрабатывает политики безопасности различных уровней, рассчитывает и разрабатывает положения о применимости механизмов контроля в контексте управления рисками информационной безопасности, соблюдает правила построения оптимальной политики безопасности в соответствии с требованиями уровня безопасности, определяет стоимость и сроки реализации проекта, работает с нормативными правовыми актами в области информационной безопасности с технической и эксплуатационной документацией, оценивает различные инструменты в области проектирования и управления информационной безопасности, соблюдает основы отечественных и зарубежных стандартов в области сертификации и аттестации объектов информатизации, учитывает основные угрозы безопасности информации и модели нарушителя в информационных системах, разрабатывает политики безопасности различных уровней, рассчитывает и разрабатывает положения о применимости механизмов контроля в контексте управления рисками информационной безопасности, формулирует научную проблему, анализирует гипотезы, проводит выбор

предмета, объекта, целей, задач исследования, создаёт эскизный, технический, рабочий проект, применяет технологии поиска, изучения, обобщения и систематизации научной информации, определяет комплекс мер для обеспечения безопасности информационных систем, составляет аналитические обзоры по вопросам обеспечения информационной безопасности систем, использует методы и средства анализа защищенности информационных систем, программные и аппаратные средства персонального компьютера для поиска и обработки информации, формулирует научную проблему, анализирует гипотезы, применяет методику создания технического задания и технического проекта при организации НИОКР, определяет порядок организации процесса исследования, методы построения оптимальных планов для научных экспериментов, оформляет научные публикации в соответствии с шаблоном IEEE, требованиями научных конференций, разрабатывает техническую документацию в соответствии с требованиями Единой системы конструкторской документации и Единой системы программной документации, анализирует получаемые результаты и формулирует выводы, выбирает и обосновывает критерии оценки защищенности открытых информационных систем, готовит научные доклады и статьи, порядок подбора классификации и систематизации информации по теме научного исследования, методы анализа и выбора решений по обеспечению требуемого уровня безопасности информационных процессов с использованием современных достижений науки в области анализ информационных процессов, защиты информации в киберфизических системах, умеет применять технологии поиска, изучения, обобщения и систематизации научной информации, методы анализа и обоснования выбора решений по обеспечению требуемого уровня безопасности информационных процессов защиты информации в киберфизических системах, владеет навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности, состав, назначение и порядок разработки политики безопасности в киберфизических системах, порядок определения уровня защищенности киберфизических систем, умеет применять современные информационные технологии, при проектировании политики безопасности вычислительных сетей в киберфизических системах, выбирать оптимальный набор организационных мер для повышения защищённости киберфизических систем, владеет навыками реализации комплекса выбранных мер, при реализации политики безопасности вычислительных сетей в киберфизических системах, навыками реализации организационно-технических мероприятий по обеспечению защиты киберфизических систем, состав системы управления информационной безопасностью киберфизических систем, порядок анализа структурно-функциональных характеристик киберфизических систем, умеет анализировать уязвимости киберфизических систем, выбирать оптимальный набор технических мер для повышения защищённости киберфизических систем, владеет навыками выбора набора организационно-технических и криптографических мер в системе информационной безопасности киберфизических систем, выбора организационно-технических мероприятий по обеспечению защиты киберфизических систем

Оценка «удовлетворительно» выставляется студенту, если студент на удовлетворительном уровне знает технологии поиска и критического анализа информации, использует методы системного подхода для решения поставленных задач с помощью цифровых и информационных технологий, организует личное цифровое пространство, осуществляет поиск, отбор и систематизацию информации для определения альтернативных вариантов стратегических решений в проблемной ситуации, выделяет и оценивает риски возможных вариантов решений проблемной ситуации, вырабатывает стратегию действий по решению проблемной ситуации, осуществляет учёт требований законодательных и правовых актов РФ, регулирующих правовые отношения в сфере информационной безопасности и защиты государственной тайны, применяет цифровые технологии для решения проектных задач, выбирая оптимальный способ их решения, исходя из действующих правовых норм и имеющихся ресурсов и ограничений, обеспечивает выполнение проекта в соответствии с установленными целями, сроками и затратами, исходя из действующих правовых норм,

имеющихся ресурсов и ограничений, в том числе с использованием цифровых инструментов, проводит контроль выполнения и оценивает эффективность реализации проекта на всех этапах его жизненного цикла, осознает свою роль в системе межличностного взаимодействия, анализирует стратегии поведения в группе, и особенности поведения разных групп людей, с которыми работает (взаимодействует), определяет статус и роль членов группы в системе межличностных отношений и учитывает на практике эти показатели, применяет методы командной работы, обеспечивает выполнение поставленных задач на основе мониторинга командной работы и своевременного реагирования на существенные отклонения, руководит выполнением поставленных задач на основе мониторинга командной работы и своевременного реагирования на существенные отклонения, руководствуется правилами деловой коммуникации в устной и письменной формах на государственном языке РФ и иностранном(ых) языке(ах), пользуется современными средствами деловой коммуникации на основе информационных технологий, осуществляет поиск и анализ требуемой информации в профессиональном взаимодействии, проводит оценку эффективности применяемых информационных технологий, решает профессиональные задачи с использованием современных коммуникационных технологий, проводит поиск необходимой информации в процессе решения стандартных коммуникативных задач на государственном(-ых) и иностранном(-ых) языках, проводит оценку эффективности применяемых коммуникативных технологий в профессиональном взаимодействии на государственном (-ых) и иностранном (-ых) языках, производит выбор оптимальных решений, учитывает культурные особенности и традиции различных социальных групп, этносов и конфессий, анализируя социальные ситуации взаимодействия, проявляет уважение к историческому наследию и социокультурным традициям различных социальных групп, опирающееся на знание этапов исторического развития России (включая основные события, основных исторических деятелей) в контексте мировой истории и ряда культурных традиций мира (в зависимости от среды и задач образования), включая мировые религии, философские и этические учения, выбирает формы, методы, приемы взаимодействия с различными социальными группами, учитывает культурные и религиозные традиции, при личном и массовом общении, определяет приемы конструктивного взаимодействия в ситуации общения, ставит цели в своей профессиональной деятельности и решает профессиональные задачи с учётом своих ресурсных возможностей и приоритетов, выбирает эффективные стратегии и тактики личностного и профессионального развития, пользуется методикой оценки эффективности применяемых методов решения поставленных задач в сфере своей профессиональной деятельности, оценивает эффективность использования времени и других ресурсов при решении поставленных задач в избранной сфере профессиональной деятельности, проводит критическую оценку эффективности использования своего времени и других ресурсов, при решении задач, поставленных в избранной сфере профессиональной деятельности, применяет методы решения задач моделирования и проектирования автоматизированных информационных систем и систем обеспечения информационной безопасности, разрабатывает и обосновывает критерии оценки эффективности проектируемой системы обеспечения информационной безопасности, разрабатывает актуальную модель угроз для автоматизированных информационных систем и учитывает её положения при формировании требований технического задания на проектируемую систему обеспечения информационной безопасности, проводит разработку и обосновывает критерии оценки эффективности проектируемой системы обеспечения информационной безопасности, оценивает эффективность решений и анализирует показатели деятельности, определяет направления развития и проблем компьютерного моделирования сложных систем, разработке и исследовании системы защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасности, реализовывает типовые задачи средствами автоматизированного и ручного функционального тестирования, учитывает направления развития технологий проектирования информационных, автоматизированных и автоматических систем, управляет коллективом исполнителей и принимает управленческие решения, соблюдает правила построения оптимальной политики безопасности в соответствии с требованиями

уровня безопасности, определяет стоимость и сроки реализации проекта, работает с нормативными правовыми актами в области информационной безопасности с технической и эксплуатационной документацией, оценивает различные инструменты в области проектирования и управления информационной безопасностью, соблюдает основы отечественных и зарубежных стандартов в области сертификации и аттестации объектов информатизации, учитывает основные угрозы безопасности информации и модели нарушителя в информационных системах, разрабатывает политики безопасности различных уровней, рассчитывает и разрабатывает положения о применимости механизмов контроля в контексте управления рисками информационной безопасности, соблюдает правила построения оптимальной политики безопасности в соответствии с требованиями уровня безопасности, определяет стоимость и сроки реализации проекта, работает с нормативными правовыми актами в области информационной безопасности с технической и эксплуатационной документацией, оценивает различные инструменты в области проектирования и управления информационной безопасностью, соблюдает основы отечественных и зарубежных стандартов в области сертификации и аттестации объектов информатизации, учитывает основные угрозы безопасности информации и модели нарушителя в информационных системах, разрабатывает политики безопасности различных уровней, рассчитывает и разрабатывает положения о применимости механизмов контроля в контексте управления рисками информационной безопасности, формулирует научную проблему, анализирует гипотезы, проводит выбор предмета, объекта, целей, задач исследования, создаёт эскизный, технический, рабочий проект, применяет технологии поиска, изучения, обобщения и систематизации научной информации, определяет комплекс мер для обеспечения безопасности информационных систем, составляет аналитические обзоры по вопросам обеспечения информационной безопасности систем, использует методы и средства анализа защищенности информационных систем, программные и аппаратные средства персонального компьютера для поиска и обработки информации, формулирует научную проблему, анализирует гипотезы, применяет методику создания технического задания и технического проекта при организации НИОКР, определяет порядок организации процесса исследования, методы построения оптимальных планов для научных экспериментов, оформляет научные публикации в соответствии с шаблоном IEEE, требованиями научных конференций, разрабатывает техническую документацию в соответствии с требованиями Единой системы конструкторской документации и Единой системы программной документации, анализирует получаемые результаты и формулирует выводы, выбирает и обосновывает критерии оценки защищенности открытых информационных систем, готовит научные доклады и статьи, порядок подбора классификации и систематизации информации по теме научного исследования, методы анализа и выбора решений по обеспечению требуемого уровня безопасности информационных процессов с использованием современных достижений науки в области анализ информационных процессов, защиты информации в киберфизических системах, умеет применять технологии поиска, изучения, обобщения и систематизации научной информации, методы анализа и обоснования выбора решений по обеспечению требуемого уровня безопасности информационных процессов защиты информации в киберфизических системах, владеет навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности, состав, назначение и порядок разработки политики безопасности в киберфизических системах, порядок определения уровня защищенности киберфизических систем, умеет применять современные информационные технологии, при проектировании политики безопасности вычислительных сетей в киберфизических системах, выбирать оптимальный набор организационных мер для повышения защищённости киберфизических систем, владеет навыками реализации комплекса выбранных мер, при реализации политики безопасности вычислительных сетей в киберфизических системах, навыками реализации организационно-технических мероприятий по обеспечению защиты киберфизических систем, состав системы управления информационной безопасностью киберфизических систем, порядок анализа структурно-

функциональных характеристик киберфизических систем, умеет анализировать уязвимости киберфизических систем, выбирать оптимальный набор технических мер для повышения защищённости киберфизических систем, владеет навыками выбора набора организационно-технических и криптографических мер в системе информационной безопасности киберфизических систем, выбора организационно-технических мероприятий по обеспечению защиты киберфизических систем

Оценка «неудовлетворительно» выставляется студенту, если студент на низком уровне знает технологии поиска и критического анализа информации, использует методы системного подхода для решения поставленных задач с помощью цифровых и информационных технологий, организует личное цифровое пространство, осуществляет поиск, отбор и систематизацию информации для определения альтернативных вариантов стратегических решений в проблемной ситуации, выделяет и оценивает риски возможных вариантов решений проблемной ситуации, вырабатывает стратегию действий по решению проблемной ситуации, осуществляет учёт требований законодательных и правовых актов РФ, регулирующих правовые отношения в сфере информационной безопасности и защиты государственной тайны, применяет цифровые технологии для решения проектных задач, выбирая оптимальный способ их решения, исходя из действующих правовых норм и имеющихся ресурсов и ограничений, обеспечивает выполнение проекта в соответствии с установленными целями, сроками и затратами, исходя из действующих правовых норм, имеющихся ресурсов и ограничений, в том числе с использованием цифровых инструментов, проводит контроль выполнения и оценивает эффективность реализации проекта на всех этапах его жизненного цикла, осознает свою роль в системе межличностного взаимодействия, анализирует стратегии поведения в группе, и особенности поведения разных групп людей, с которыми работает (взаимодействует), определяет статус и роль членов группы в системе межличностных отношений и учитывает на практике эти показатели, применяет методы командной работы, обеспечивает выполнение поставленных задач на основе мониторинга командной работы и своевременного реагирования на существенные отклонения, руководит выполнением поставленных задач на основе мониторинга командной работы и своевременного реагирования на существенные отклонения, руководствуется правилами деловой коммуникации в устной и письменной формах на государственном языке РФ и иностранном(ых) языке(ах), пользуется современными средствами деловой коммуникации на основе информационных технологий, осуществляет поиск и анализ требуемой информации в профессиональном взаимодействии, проводит оценку эффективности применяемых информационных технологий, решает профессиональные задачи с использованием современных коммуникационных технологий, проводит поиск необходимой информации в процессе решения стандартных коммуникативных задач на государственном(-ых) и иностранном(-ых) языках, проводит оценку эффективности применяемых коммуникативных технологий в профессиональном взаимодействии на государственном (-ых) и иностранном (-ых) языках, производит выбор оптимальных решений, учитывает культурные особенности и традиции различных социальных групп, этносов и конфессий, анализируя социальные ситуации взаимодействия, проявляет уважение к историческому наследию и социокультурным традициям различных социальных групп, опирающееся на знание этапов исторического развития России (включая основные события, основных исторических деятелей) в контексте мировой истории и ряда культурных традиций мира (в зависимости от среды и задач образования), включая мировые религии, философские и этические учения, выбирает формы, методы, приемы взаимодействия с различными социальными группами, учитывает культурные и религиозные традиции, при личном и массовом общении, определяет приемы конструктивного взаимодействия в ситуации общения, ставит цели в своей профессиональной деятельности и решает профессиональные задачи с учётом своих ресурсных возможностей и приоритетов, выбирает эффективные стратегии и тактики личностного и профессионального развития, пользуется методикой оценки эффективности применяемых методов решения поставленных задач в сфере своей профессиональной деятельности, оценивает эффективность использования времени и других ресурсов при решении поставленных задач в избранной сфере

профессиональной деятельности, проводит критическую оценку эффективности использования своего времени и других ресурсов, при решении задач, поставленных в избранной сфере профессиональной деятельности, применяет методы решения задач моделирования и проектирования автоматизированных информационных систем и систем обеспечения информационной безопасности, разрабатывает и обосновывает критерии оценки эффективности проектируемой системы обеспечения информационной безопасности, разрабатывает актуальную модель угроз для автоматизированных информационных систем и учитывает её положения при формировании требований технического задания на проектируемую систему обеспечения информационной безопасности, проводит разработку и обосновывает критерии оценки эффективности проектируемой системы обеспечения информационной безопасности, оценивает эффективность решений и анализирует показатели деятельности, определяет направления развития и проблем компьютерного моделирования сложных систем, разработке и исследовании системы защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасности, реализовывает типовые задачи средствами автоматизированного и ручного функционального тестирования, учитывает направления развития технологий проектирования информационных, автоматизированных и автоматических систем, управляет коллективом исполнителей и принимает управленческие решения, соблюдает правила построения оптимальной политики безопасности в соответствии с требованиями уровня безопасности, определяет стоимость и сроки реализации проекта, работает с нормативными правовыми актами в области информационной безопасности с технической и эксплуатационной документацией, оценивает различные инструменты в области проектирования и управления информационной безопасностью, соблюдает основы отечественных и зарубежных стандартов в области сертификации и аттестации объектов информатизации, учитывает основные угрозы безопасности информации и модели нарушителя в информационных системах, разрабатывает политики безопасности различных уровней, рассчитывает и разрабатывает положения о применимости механизмов контроля в контексте управления рисками информационной безопасности, соблюдает правила построения оптимальной политики безопасности в соответствии с требованиями уровня безопасности, определяет стоимость и сроки реализации проекта, работает с нормативными правовыми актами в области информационной безопасности с технической и эксплуатационной документацией, оценивает различные инструменты в области проектирования и управления информационной безопасностью, соблюдает основы отечественных и зарубежных стандартов в области сертификации и аттестации объектов информатизации, учитывает основные угрозы безопасности информации и модели нарушителя в информационных системах, разрабатывает политики безопасности различных уровней, рассчитывает и разрабатывает положения о применимости механизмов контроля в контексте управления рисками информационной безопасности, формулирует научную проблему, анализирует гипотезы, проводит выбор предмета, объекта, целей, задач исследования, создаёт эскизный, технический, рабочий проект, применяет технологии поиска, изучения, обобщения и систематизации научной информации, определяет комплекс мер для обеспечения безопасности информационных систем, составляет аналитические обзоры по вопросам обеспечения информационной безопасности систем, использует методы и средства анализа защищенности информационных систем, программные и аппаратные средства персонального компьютера для поиска и обработки информации, формулирует научную проблему, анализирует гипотезы, применяет методику создания технического задания и технического проекта при организации НИОКР, определяет порядок организации процесса исследования, методы построения оптимальных планов для научных экспериментов, оформляет научные публикации в соответствие с шаблоном IEEE, требованиями научных конференций, разрабатывает техническую документацию в соответствии с требованиями Единой системы конструкторской документации и Единой системы программной документации, анализирует получаемые результаты и формулирует выводы, выбирает и обосновывает критерии оценки защищенности открытых информационных систем, готовит научные доклады и статьи, порядок подбора классификации и систематизации

информации по теме научного исследования, методы анализа и выбора решений по обеспечению требуемого уровня безопасности информационных процессов с использованием современных достижений науки в области анализ информационных процессов, защиты информации в киберфизических системах, умеет применять технологии поиска, изучения, обобщения и систематизации научной информации, методы анализа и обоснования выбора решений по обеспечению требуемого уровня безопасности информационных процессов защиты информации в киберфизических системах, владеет навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности, состав, назначение и порядок разработки политики безопасности в киберфизических системах, порядок определения уровня защищенности киберфизических систем, умеет применять современные информационные технологии, при проектировании политики безопасности вычислительных сетей в киберфизических системах, выбирать оптимальный набор организационных мер для повышения защищенности киберфизических систем, владеет навыками реализации комплекса выбранных мер, при реализации политики безопасности вычислительных сетей в киберфизических системах, навыками реализации организационно-технических мероприятий по обеспечению защиты киберфизических систем, состав системы управления информационной безопасностью киберфизических систем, порядок анализа структурно-функциональных характеристик киберфизических систем, умеет анализировать уязвимости киберфизических систем, выбирать оптимальный набор технических мер для повышения защищенности киберфизических систем, владеет навыками выбора набора организационно-технических и криптографических мер в системе информационной безопасности киберфизических систем, выбора организационно-технических мероприятий по обеспечению защиты киберфизических систем

4. Типовые контрольные задания или иные материалы, необходимые для оценки результатов освоения образовательной программы

4.1 Вопросы к итоговому (государственному) экзамену

4.1.1 Теоретические вопросы

I Теоретические основы компьютерной безопасности:

1. Содержание и структура понятия компьютерной безопасности.
2. Общая характеристика принципов, методов и механизмов обеспечения компьютерной безопасности.
3. Понятие политики и моделей безопасности информации в компьютерных системах.
4. Общая характеристика политики дискреционного доступа.
5. Общая характеристика моделей полномочного (мандатного) доступа.
6. Общая характеристика тематического разграничения доступа.
7. Тематическая решетка мультирубрик иерархического рубрикатора.
8. Модели тематико-иерархического разграничения доступа.
9. Понятие и общая характеристика скрытых каналов утечки информации.
10. Методы защиты информации от утечки по побочным каналам излучений.
11. Теоретико-информационные модели невыводимости и невливания (невмешательства).
12. Общая характеристика моделей и технологий обеспечения целостности данных.
13. Технологии электронной подписи.
14. Резервирование архивирование и журнализация данных.
15. Технологии и системы репликации данных.
16. Общие положения о политике безопасности в распределенных КС
17. Зональная модель безопасности в распределенных КС.
18. Общая характеристика измерения (оценки) эмпирических объектов.
19. Стандартизация требований к архитектуре, функциям и критериям оценки подсистем безопасности в АИС.

20. Показатели защищенности СВТ/СУБД и классификация АС/АИС по требованиям защиты от НСД к информации.

21. Критерии оценки безопасности информационных технологий. Профили защиты СУБД.

22. Модели комплексной оценки защищенности КС.

23. Теоретико-графовая модель систем индивидуально-группового доступа к иерархически организованным информационным ресурсам.

II. Технологии обеспечения информационной безопасности:

1. Сущность и понятие информационной безопасности.

2. Значение информационной безопасности и ее место в системе национальной безопасности.

3. Современная доктрина информационной безопасности Российской Федерации.

4. Сущность и понятие защиты информации.

5. Цели и значение защиты информации.

6. Теоретические и концептуальные основы защиты информации.

7. Организационные основы и методологические принципы защиты информации.

8. Современные факторы, влияющие на защиту информации.

9. Критерии, условия и принципы отнесения информации к защищаемой.

10. Состав и классификация носителей защищаемой информации.

11. Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности.

12. Классификация защищаемой информации по собственникам и владельцам.

13. Понятие и структура угроз защищаемой информации.

14. Источники, виды и способы дестабилизирующего воздействия на защищаемую информацию.

15. Причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию.

16. Каналы и методы несанкционированного доступа к конфиденциальной информации.

17. Направления, виды и особенности деятельности разведывательных служб по несанкционированному доступу к конфиденциальной информации.

18. Объекты защиты информации.

19. Классификация видов, методов и средств защиты информации.

20. Кадровое и ресурсное обеспечение защиты информации.

21. Технологическое обеспечение защиты информации.

22. Назначение и структура систем защиты информации.

23. Аудит информационной безопасности объекта.

24. Оценка информационной безопасности объекта.

25. Комплексная система защиты информации объекта.

III. Криптографические методы защиты информации:

1. Угрозы безопасности операционной системы. Понятие защищенной операционной системы.

2. Структура системы обеспечения информационной безопасности.

3. Принципы организации технического, программного и информационного обеспечения. Этапы построения защиты.

4. Субъекты, объекты, методы и права доступа, привилегии субъекта доступа.

5. Дискреционное управление доступом. Изолированная программная среда. Мандатное управление доступом.

6. Контроль информационных потоков. Идентификация, аутентификация и авторизация.

7. Парольная аутентификация в операционных системах семейства Windows и UNIX.

8. Аутентификация на основе внешних носителей ключа. Биометрическая аутентификация: общая схема, преимущества, проблемы.

9. Управление доступом в операционных системах семейства Windows и UNIX.

10. Аудит. Требования к подсистеме аудита.
 11. Необходимость аудита в защищенной системе. Реализация аудита в операционных системах семейства Windows и UNIX.
 12. Домены Windows. Преимущества доменной архитектуры локальной сети. Понятие домена, контроллер домена.
 13. Сетевые атаки. Стадии проведения сетевой атаки.
 14. Классификации сетевых угроз, уязвимостей и атак. Примеры типичных сетевых атак.
 15. Методы перехвата сетевых соединений в сетях TCP/IP. Десинхронизация TCP-соединений. Атаки, направленные на маршрутизаторы. Несанкционированный обмен данными.
 16. Технические меры защиты от сетевых атак.
 17. Криптографические протоколы аутентификации.
 18. Разработка защищенных сетевых приложений.
 19. Средства защиты локальных сетей при подключении к Интернет. Межсетевые экраны (МЭ).
 20. Аудит. Средства обеспечения защиты информации в СУБД и многоуровневая защита.
 21. Политика безопасности в СУБД. Модели безопасности в СУБД.
 22. Угрозы конфиденциальности СУБД.
 23. Криптографические методы защиты баз данных.
 24. Угрозы целостности СУБД.
 25. Основные виды и причины возникновения угроз целостности. Способы противодействия. Понятие транзакции. Блокировки. Ссылочно целостность. Правила (триггеры).
- IV. Основы научных исследований:
1. Наука, ее особенности и критерии. Социальные функции науки.
 2. Научные исследования: сущность и особенности. Классификация научных исследований.
 3. Организация научных исследований в РФ. Структура научного знания. Формы научного знания.
 4. Методы научного исследования, их классификация. Основные этапы проведения научно-исследовательской работы.
 5. Планирование научно-исследовательской работы.
 6. Характеристика структурных компонентов программы научного исследования.
 7. Определение объекта и предмета исследования. Определение цели и задач исследования
 8. Характеристика методологического раздела программы исследования
 9. Основные источники научной информации, их классификация.
 10. Виды научных изданий. Виды учебных изданий. Справочно-информационные издания.
 11. Систематизация научной информации. Методика чтения научной литературы.
 12. Реферат как научное произведение, его назначение и структура.
 13. Курсовая работа.
 14. Магистерская диссертация. Научный доклад, его назначение и структура. Тезисы доклада.
 15. Научная статья, ее структура и содержание.
 16. Структура научной работы, ее основные композиционные элементы.
 17. Оформление библиографического аппарата научной работы.

18. Использование современных информационных технологий при поиске и изучении литературных источников.

19. Роль информационных технологий в презентации результатов научных исследований.

4.1.2 Практические вопросы

1. Смоделировать в программе «Electronics Workbench» и исследовать сигнальные демаскирующие признаки амплитудно-модулированных и частотно-модулированных сигналов.

2. Смоделировать в программе «Electronics Workbench» и исследовать сигнальные демаскирующие признаки амплитудно-манипулированных, частотно-манипулированных сигналов и фазово-манипулированных сигналов.

3. Собрать схему и провести исследования зависимости величины опасного сигнала акустоэлектрического преобразователя от площади диффузора акустоэлектрического преобразователя (динамика) и от интенсивности входного акустического сигнала.

4. Собрать схему и провести исследования зависимости величины опасного сигнала акустоэлектрического преобразователя от расстояния между источником акустического сигнала и акустоэлектрическим преобразователем и от угла прихода звуковой волны.

5. Смоделировать в программе «Electronics Workbench» и исследовать сигнальные демаскирующие признаки GMSK сигнала.

6. Смоделировать и исследовать в программе «Electronics Workbench» электрические схемы замещения эффекта паразитной генерации на транзисторном усилителе и логических элементах.

7. Смоделировать и исследовать в программе «Electronics Workbench» электрическую схему замещения электрического канала утечки информации, возникающего путем наводки информационного сигнала в соединительную линию ВТСС за счет паразитной связи.

8. Смоделировать и исследовать в программе «Electronics Workbench» электрическую схему замещения системы высокочастотного навязывания.

9. Смоделировать и исследовать в программе «Electronics Workbench» электрические схемы замещения кабельного радара в режиме измерения различных неоднородностей, создаваемых подключением электронных устройств негласного перехвата информации.

10. Смоделировать и исследовать в программе «Electronics Workbench» электрическую схему замещения электромагнитного технического канала утечки информации, возникающего за счёт ПЭМИ от средств вычислительной техники.

11. Смоделировать и исследовать в программе «Electronics Workbench» электрическую схему замещения стетоскопа.

12. Смоделировать и исследовать в программе «Electronics Workbench» электрическую схему радиозакладного устройства.

13. Смоделировать и исследовать в программе «Electronics Workbench» электрическую схему замещения процесса паразитной модуляции на нелинейном элементе.

14. Смоделировать в программе «Electronics Workbench» и провести исследование свойств интегрирующей и дифференцирующих RC и RL цепей.

15. Смоделировать в программе «Electronics Workbench» и провести исследование резонансных свойств последовательного и параллельного колебательных контуров.

16. Смоделировать и исследовать в программе «Mathcad» электрическое поле от дискретного набора электрических зарядов.

17. Смоделировать и исследовать в программе «Mathcad» магнитное поле от дискретного набора постоянных электрических токов.

18. Смоделировать и исследовать в программе «Mathcad» параметры плоской электромагнитной волны.

19. Смоделировать в программе «Electronics Workbench» и исследовать эквивалентную

- схему замещения внешней емкостной параллельной паразитной связи между двумя каналами
20. Собрать лабораторную установку и провести исследование способа зашумления радиозакладок при помощи генератора шума «ГШ – 1000М».
21. Собрать лабораторную установку и провести исследования звукопоглощающих и звукоизолирующих свойств материалов.
22. Смоделировать и исследовать в программе «Electronics Workbench» принципы построения и работы амплитудного диодного ограничителя для защиты телефонного аппарата.
23. Смоделировать и исследовать в программе «Electronics Workbench» принципы построения и работы схем защиты микрофонной и звонковой цепей телефонного аппарата.
24. Смоделировать в программе «Electronics Workbench» и исследовать эквивалентную схему замещения последовательной паразитной связи через паразитную взаимную индуктивность между двумя каналами.
25. Смоделировать в программе «Electronics Workbench» и исследовать эквивалентную схему замещения процесса экранирования источника электромагнитного излучения.
26. Смоделировать в программе «Electronics Workbench» и исследовать эквивалентную схему замещения процесса экранирования коаксиального кабеля.
27. Смоделировать в программе «Electronics Workbench» и исследовать принципы работы пассивных фильтров низких и высоких частот.
28. Смоделировать в программе «Electronics Workbench» и исследовать принципы работы пассивных полосно-пропускающих и полосно-заграждающих фильтров.
29. Программно исследовать эффективность маскировки звуков при воздействии тонального маскирующего звука, белого и розового шумов
30. Смоделировать и исследовать в программе «Electronics Workbench» принципы построения и работы схемы фильтрации опасных сигналов для защиты телефонной линии.
31. Смоделировать и исследовать в программе «Electronics Workbench» принципы построения комбинированной схему защиты телефонного аппарата.
32. Провести в программе «WAV Scrambler» исследование принципов работы скремблера в режиме временной и частотной инверсии.
33. Провести в программе «WAV Scrambler» исследование принципов работы скремблера в режиме временного и частотного скремблирования.
34. Смоделировать и исследовать в программе «Electronics Workbench» принцип работы емкостного акустоэлектрического преобразователя.
35. Смоделировать и исследовать в программе «Electronics Workbench» принцип работы индуктивного акустоэлектрического преобразователя.
36. Смоделировать и исследовать в программе «Electronics Workbench» принцип работы пьезоэлектрического акустоэлектрического преобразователя.
37. Смоделировать в программах «MathCAD» и «Electronics Workbench» с помощью элементов с сосредоточенными параметрами сегмент длинной линии в виде витой пары пятой категории и провести ее исследование.

4.2 Оценочные средства для выпускной квалификационной работы

4.2.1 Перечень тем выпускных квалификационных работ

Направление деятельности	Примерная тематика
эксплуатационная деятельность: – установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований,	– Разработка проекта комплексной безопасности производственного предприятия. – Организация системы защиты персональных данных в «Ставропольпромстройбанк ОАО». – Разработка информационной системы хранения медиаконтента телевизионного канала «СТВ плюс». – Разработка защищенной корпоративной сети

– участие в проведении аттестации объектов, помещений, технических средств, систем, программ и алгоритмов на предмет соответствия требованиям защиты информации, – администрирование подсистем информационной безопасности объекта,	предприятия ООО «Бестсофт» на базе аппаратно-программного комплекса шифрования «Континент». – Разработка проекта системы видеонаблюдения для офисного здания ООО «Консалт-Трейд». – Разработка рекомендаций по реализации технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. – Разработка рекомендаций по применению многофункционального поискового прибора «ST033 Пиранья» для проведения оперативных мероприятий по обнаружению и локализации технических средств негласного получения информации на объекте информатизации. – Разработка рекомендаций по снижению риска утечки конфиденциальной информации по техническим каналам предприятия.
– проектно-технологическая деятельность: – сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности, – проведение проектных расчетов элементов систем обеспечения информационной безопасности, – участие в разработке технологической и эксплуатационной документации, – проведение предварительного технико-экономического обоснования проектных расчетов	– Разработка проекта защищенной беспроводной локальной сети организации с использованием сервера RADIUS. – Разработка модели угроз информации для распределенной вычислительной сети организации. – Разработка пакета организационно-распорядительной документации по обеспечению безопасности персональных данных для высшего учебного заведения. – Разработка технических решений по созданию интегрированной системы безопасности предприятия на основе оборудования компании «Стилсофт». – Разработка подсистемы информационной безопасности для аппаратно-программного комплекса Системы 112. – Разработка проекта системы контроля и управления доступом в ГУП СК «Аэропорт Ставрополь». – Разработка политики разграничения доступа на предприятии. – Разработка способа защищённого информационного обмена в беспроводных системах передачи информации с кодовым разделением каналов. – Разработка проекта защищенной распределенной сети ООО «Оргстекло-Юг» с использованием технологии VPN.
– экспериментально-исследовательская деятельность: – сбор, изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования,	– Разработка мероприятий по защите информации в корпоративной сети организации. – Разработка проекта защищенной распределенной сети организации с использованием АПКШ «Континент». – Разработка рекомендаций по внедрению средств

– проведение экспериментов по заданной методике, обработка и анализ результатов, – проведение вычислительных экспериментов с использованием стандартных программных средств,	обеспечения дополнительной аутентификации и криптографической защиты в корпоративной сети организации. – Разработка проекта защищенной вычислительной сети организации с использованием средств межсетевого экранирования. – Разработка интегрированной системы охраны предприятия. – Разработка методики поиска уязвимостей компьютерной сети предприятия. – Разработка комплекса мероприятий по защите объекта от утечки акустической информации. – Разработка рекомендаций по внедрению систем видеонаблюдения в малых предприятиях. – Разработка рекомендаций по обеспечению безопасности персональных данных для высшего учебного заведения.
– организационно-управленческая деятельность: – осуществление организационно-правового обеспечения информационной безопасности объекта защиты, – организация работы малых коллективов исполнителей с учетом требований защиты информации, – совершенствование системы управления информационной безопасностью, – изучение и обобщение опыта работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации и сохранения государственной и других видов тайны, – контроль эффективности реализации политики информационной безопасности объекта.	– Разработка методических рекомендаций по прогнозированию чрезвычайных ситуаций в системах оповещения населения. – Разработка рекомендаций по применению устройство защиты телефонных линий «МП-7 Гвард» и «МП-8 Сигма-РА» для защиты от несанкционированного доступа и утечки информации из выделенных помещений. – Разработка рекомендаций по применению комплекса радиомониторинга и цифрового анализа сигналов «Кассандра К21» для выявления несанкционированных радиоизлучений. – Разработка технических решений по созданию комплексной системы энергетического скрытия конфиденциальной информации для предотвращения ее утечки по техническим каналам. – Разработка рекомендаций по организации защищенных параллельных вычислений в системах обработки данных. – Разработка рекомендаций по применению программно-аппаратного комплекса «Спрут-мини-А» для проверки выполнения норм эффективности защиты речевой информации в выделенном помещении. – Разработка системы видеонаблюдения организации с использованием IP-видеокамер.

4.2.2 Структура работы

Раздел 1. Проведение предпроектного обследования предприятия

Уровень обученности	Формулировка задания	Оцениваемые компетенции
---------------------	----------------------	-------------------------

Знать: новые методы исследования в профессиональной деятельности, направления развития информационных технологий, методы разработки систем, комплексов, средств и технологий обеспечения информационной безопасности, способы проведения обоснования состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов, программы и методики испытаний средств и систем обеспечения информационной безопасности, методы анализа фундаментальных и прикладных проблем информационной безопасности в условиях становления.	Задание 1. Объект и методы проведения предпроектного обследования, программа проведения обследования, план-график выполнения работ на стадии сбора материалов обследования.	ПК-1	ПК-2	ПК-3,	ПК-4
	Задание 2. Изучение и описание Общая характеристика предприятия (организации), организационная структура предприятия, группы функциональных задач и подзадач, организационно-управленческая модель	ПК-1	ПК-2	ПК-3,	ПК-4
	Задание 3. Анализ структуры, направления деятельности и организации системы защиты информации объекта исследования. Анализ ценных активов предприятия с целью обоснования необходимости проведения исследований.	ПК-1	ПК-2	ПК-3,	ПК-4
	Задание 4. Проведение оценки риска информационной безопасности предприятия с целью формирования направлений модернизации системы защиты информации объекта исследований. Выбор методов и средств модернизации системы защиты информации предприятия. Обоснование направлений исследования	ПК-1	ПК-2	ПК-3,	ПК-4
Уметь: применять новые методы исследования в профессиональной деятельности, анализировать направления развития информационных технологий, применять методы разработки систем, комплексов, средств и технологий обеспечения информационной безопасности, проводить обоснования состава, характеристик и функциональных	Задание 1. Объект и методы проведения предпроектного обследования, программа проведения обследования, план-график выполнения работ на стадии сбора материалов обследования.	ПК-1	ПК-2	ПК-3,	ПК-4
	Задание 2. Изучение и описание Общая характеристика предприятия (организации),	ПК-1	ПК-2	ПК-3,	ПК-4

возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов, применять программы и методики испытаний средств и систем обеспечения информационной безопасности,	организационная структура предприятия, группы функциональных задач и подзадач, организационно-управленческая модель				
	Задание 3. Анализ структуры, направления деятельности и организации системы защиты информации объекта исследования. Анализ ценных активов предприятия с целью обоснования необходимости проведения исследований.	ПК-1	ПК-2	ПК-3,	ПК-4
	Задание 4. Проведение оценки риска информационной безопасности предприятия с целью формирования направлений модернизации системы защиты информации объекта исследований. Выбор методов и средств модернизации системы защиты информации предприятия. Обоснование направлений исследования	ПК-1	ПК-2	ПК-3,	ПК-4
Владеть: способностью к абстрактному мышлению, анализу, синтезу, самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения, способностью к коммуникации в устной и письменной формах на государственном и одном из иностранных языков для решения задач профессиональной деятельности, к самостоятельному обучению и применению новых методов исследования профессиональной деятельности, способностью анализировать направления развития информационных технологий, прогнозировать эффективность, разрабатывать системы, комплексы, средства и технологии обеспечения	Задание 1. Объект и методы проведения предпроектного обследования, программа проведения обследования, план-график выполнения работ на стадии сбора материалов обследования.	ПК-1	ПК-2	ПК-3,	ПК-4
	Задание 2. Изучение и описание Общая характеристика предприятия (организации), организационная структура предприятия, группы функциональных задач и подзадач, организационно-управленческая модель	ПК-1	ПК-2	ПК-3,	ПК-4
	Задание 3. Анализ структуры, направления деятельности и организации системы защиты информации объекта исследования. Анализ ценных активов предприятия с целью обоснования необходимости проведения исследований.	ПК-1	ПК-2	ПК-3,	ПК-4

информационной безопасности, проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов	Задание 4. Проведение оценки риска информационной безопасности предприятия с целью формирования направлений модернизации системы защиты информации объекта исследований. Выбор методов и средств модернизации системы защиты информации предприятия. Обоснование направлений исследования	ПК-1	ПК-2	ПК-3,	ПК-4
--	---	------	------	-------	------

Раздел 2. Реализация проектируемой информационной системы (подсистемы)

Уровень обученности	Формулировка задания	Оцениваемые компетенции			
– Знать: методику сбора, обработки, анализа и систематизации научно-технической информации по теме исследования, выбора методов, методы проведения экспериментальных исследований защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента, методы обработки результатов экспериментальных исследований, методику проведения аудита информационной безопасности информационных систем и объектов информатизации, методики проведения занятий по избранным дисциплинам предметной области данного направления и разработки методических материалов, используемых в образовательной деятельности.	Задание 1. Проведение выбора требуемых для реализации задач исследования, на основе анализа существующих методов и средств защиты информации по выбранному направлению, с учётом требований нормативных документов.	ПК-1	ПК-2	ПК-3,	ПК-4
	Задание 2. Разработка предложений по реализации предложенных мероприятий. Построение математических моделей структурных элементов системы защиты информации предприятия.	ПК-1	ПК-2	ПК-3,	ПК-4
	Задание 3. Проведение необходимых расчётов и графических построений. Построение алгоритмов и разработка программных продуктов.	ПК-1	ПК-2	ПК-3,	ПК-4
	Задание 4. Сравнительный анализ предлагаемых средств защиты информации.	ПК-1	ПК-2	ПК-3,	ПК-4
Уметь: применять методы анализа фундаментальных и прикладных проблем информационной безопасности в условиях становления, методику сбора, обработки, анализа и систематизации научно-технической информации по теме исследования, выбирать методики проведения	Задание 1. Проведение выбора требуемых для реализации задач исследования, на основе анализа существующих методов и средств защиты информации по выбранному направлению, с учётом требований нормативных	ПК-1	ПК-2	ПК-3,	ПК-4

экспериментальных исследований защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента, применять методы обработки результатов экспериментальных исследований, методику проведения аудита информационной безопасности информационных систем и объектов информатизации, методики проведения занятий по избранным дисциплинам предметной области данного направления и разработки методических материалов, используемых в образовательной деятельности.	документов.				
	Задание 2. Разработка предложений по реализации предложенных мероприятий. Построение математических моделей структурных элементов системы защиты информации предприятия.	ПК-1	ПК-2	ПК-3,	ПК-4
	Задание 3. Проведение необходимых расчётов и графических построений. Построение алгоритмов и разработка программных продуктов.	ПК-1	ПК-2	ПК-4	ПК-6
	Задание 4. Сравнительный анализ предлагаемых средств защиты информации	ПК-1	ПК-2	ПК-3,	ПК-4
Владеть: навыками разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности, анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления, осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методов, проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента, обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи, проводить аудит информационной безопасности информационных систем и объектов информатизации, проводить аттестацию объектов информатизации по требованиям безопасности информации, проводить занятия по избранным дисциплинам предметной области	Задание 1. Проведение выбора требуемых для реализации задач исследования, на основе анализа существующих методов и средств защиты информации по выбранному направлению, с учётом требований нормативных документов.	ПК-1	ПК-2	ПК-3,	ПК-4
	Задание 2. Разработка предложений по реализации предложенных мероприятий. Построение математических моделей структурных элементов системы защиты информации предприятия.	ПК-1	ПК-2	ПК-3,	ПК-4
	Задание 3. Проведение необходимых расчётов и графических построений. Построение алгоритмов и разработка программных продуктов.	ПК-1	ПК-2	ПК-3,	ПК-4
	Задание 4. Сравнительный анализ предлагаемых средств защиты информации.	ПК-1	ПК-2	ПК-3,	ПК-4

данного направления и разрабатывать методические материалы, используемые в образовательной деятельности,					
--	--	--	--	--	--

Графический материал (при необходимости): диаграммы сравнительного анализа, структурные, функциональные и принципиальные электрические схемы, листинги программ, блок-схемы алгоритмов, топология сети и т. д.

Раздел 3. Оценка эффективности предложенных рекомендаций (мероприятий)

Уровень обученности	Формулировка задания	Оцениваемые компетенции			
Знать: методики управления коллективом исполнителей и принятия управленческих решений, методы организации управления информационной безопасностью, нормативные акты и нормативные методические документы ФСБ России, ФСТЭК России, порядок выполнения работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности, порядок разработки проектов, организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности	Задание 1 Выбор критериев и проведение оценки эффективности реализации разработанных рекомендаций.	ПК-1	ПК-2	ПК-3,	ПК-4
	Задание 2 Проведение технико-экономического обоснования целесообразности и реализуемости разработанных рекомендаций	ПК-1	ПК-2	ПК-5	ПК-6
	Задание 3 Оценка экологичности проекта. Анализ перспектив развития методов и средств защиты информации по выделенному направлению.	ПК-1	ПК-2	ПК-3,	ПК-4
Уметь применять методики управления коллективом исполнителей и принятия управленческих решений, методы организации управления информационной безопасностью, нормативные акты и нормативные методические документы ФСБ России, ФСТЭК России, уметь выполнять работы по вводу в эксплуатацию систем и средств обеспечения информационной безопасности, разрабатывать проекты, организационно-распорядительные документы, бизнес-планы в сфере профессиональной деятельности	Задание 1 Выбор критериев и проведение оценки эффективности реализации разработанных рекомендаций.	ПК-1	ПК-2	ПК-3,	ПК-4
	Задание 2 Проведение технико-экономического обоснования целесообразности и реализуемости разработанных рекомендаций	ПК-1	ПК-2	ПК-5	ПК-6
	Задание 3 Оценка экологичности проекта. Анализ перспектив развития методов и средств защиты информации по выделенному направлению.	ПК-1	ПК-2	ПК-3,	ПК-4
Владеть: способностью организовать выполнение работ, управлять коллективом исполнителей и принимать управленческие решения, организовать управление	Задание 1 Выбор критериев и проведение оценки эффективности реализации разработанных рекомендаций.	ПК-1	ПК-2	ПК-3,	ПК-4
	Задание 2 Проведение технико-экономического	ПК-1	ПК-2	ПК-5	ПК-6

информационной безопасностью, организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России, организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности, способностью разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности	обоснования целесообразности и реализуемости разработанных рекомендаций				
	Задание 3 Оценка эффективности предложенных рекомендаций и технико-экономическое обоснование принятых решений.	ПК-1	ПК-2	ПК-3,	ПК-4

5. Методические материалы, определяющие процедуры оценивания результатов освоения образовательной программы

5.1 Методические материалы, определяющие процедуры оценивания результатов освоения образовательной программы на итоговом (государственном) экзамене

Процедура проведения государственного экзамена осуществляется в соответствии с Положением о порядке проведения государственной итоговой аттестации по образовательным программам высшего образования - программам бакалавриата, программам специалитета и программам магистратуры в СКФУ.

В экзаменационный билет включаются: три вопроса (2 теоретических и 1 практический).

Каждый обучающийся самостоятельно выбирает экзаменационный билет один раз посредством произвольного извлечения. Номер билета фиксируется секретарем ГЭК в соответствующем протоколе.

На подготовку к ответу на экзаменационный билет студенту отводится 1 час. При подготовке студент имеет право пользоваться программой государственного экзамена, а также с разрешения ГЭК - справочной литературой.

При проверке практического задания, оцениваются: практические навыки студента и уровень владения компетенциями.

5.2 Методические материалы, определяющие процедуры оценивания результатов освоения образовательной программы на защите выпускной квалификационной работы / научного доклада

На каждом этапе осуществляется текущий контроль за процессом формирования компетенций. Предлагаемые обучающемуся задания позволяют проверить компетенции ПК-1, ПК-2, ПК-3, ПК-4. При защите **выпускной квалификационной работы** оцениваются:

1. Пояснительная записка ВКР:

- уровень и характер раскрытия актуальности магистерского исследования, методологической обоснованности, теоретической разработанности, достоверности полученных результатов,

- логика и стиль изложения результатов исследования,

- соответствие работы направлению подготовки, установленным требованиям к оформлению работы,

- семантическое содержание пояснительной записки,

- текстуально-иллюстративное оформление пояснительной записки в соответствии с требованиями методических рекомендаций.

2. Доклад студента (в т.ч. наличие презентации, раздаточного материала и т.д.) и аргументированность ответа на вопросы членов комиссии и замечания рецензента.

3. Отзыв научного руководителя.

3. Оценка работы рецензентом.

Дополнительным показателем является наличие справки о результатах внедрения решений, разработанных в ВКР.

15. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ЧЛЕНАМ ГОСУДАРСТВЕННОЙ ЭКЗАМЕНАЦИОННОЙ КОМИССИИ ПО УЧАСТИЮ В ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

1. Перечень компетенций, знаний, умений, владений, уровень усвоения которых должен быть проверен на государственном экзамене

Цели и задачи государственного экзамена в соответствии с требованиями ФГОС ВО по направлению 10.04.01 «Информационная безопасность» состоят в выявлении уровня теоретической подготовки специалиста и степени его подготовленности к профессиональной деятельности в области информационной безопасности.

Выпускник магистратуры по направлению подготовки «Информационная безопасность» на высоком уровне: подбирает технологии поиска и критического анализа информации, использует методы системного подхода для решения поставленных задач с помощью цифровых и информационных технологий, организует личное цифровое пространство, осуществляет поиск, отбор и систематизацию информации для определения альтернативных вариантов стратегических решений в проблемной ситуации, выделяет и оценивает риски возможных вариантов решений проблемной ситуации, вырабатывает стратегию действий по решению проблемной ситуации, осуществляет учёт требований законодательных и правовых актах РФ, регулирующих правовые отношения в сфере информационной безопасности и защиты государственной тайны, применяет цифровые технологии для решения проектных задач, выбирая оптимальный способ их решения, исходя из действующих правовых норм и имеющихся ресурсов и ограничений, обеспечивает выполнение проекта в соответствии с установленными целями, сроками и затратами, исходя из действующих правовых норм, имеющихся ресурсов и ограничений, в том числе с использованием цифровых инструментов, проводит контроль выполнения и оценивает эффективность реализации проекта на всех этапах его жизненного цикла, осознает свою роль в системе межличностного взаимодействия, анализирует стратегии поведения в группе, и особенности поведения разных групп людей, с которыми работает (взаимодействует), определяет статус и роль членов группы в системе межличностных отношений и учитывает на практике эти показатели, применяет методы командной работы, обеспечивает выполнение поставленных задач на основе мониторинга командной работы и своевременного реагирования на существенные отклонения, руководит выполнением поставленных задач на основе мониторинга командной работы и своевременного реагирования на существенные отклонения, руководствуется правилами деловой коммуникации в устной и письменной формах на государственном языке РФ и иностранном(ых) языке(ах), пользуется современными средствами деловой коммуникации на основе информационных технологий, осуществляет поиск и анализ требуемой информации в профессиональном взаимодействии, проводит оценку эффективности применяемых информационных технологий, решает профессиональные задачи с использованием современных коммуникационных технологий, проводит поиск необходимой информации в процессе решения стандартных коммуникативных задач на государственном(-ых) и иностранном(-ых) языках, проводит оценку эффективности применяемых коммуникативных технологий в профессиональном взаимодействии на государственном (-ых) и иностранном (-ых) языках, производит выбор оптимальных решений, учитывает культурные особенности и традиции различных социальных групп, этносов и конфессий, анализируя социальные ситуации взаимодействия, проявляет уважение к историческому наследию и социокультурным традициям различных социальных групп, опирающееся на знание этапов исторического развития России (включая основные события, основных исторических деятелей) в контексте мировой истории и ряда культурных традиций мира (в зависимости от среды и задач образования), включая мировые религии, философские и этические учения, выбирает формы, методы, приемы взаимодействия с

различными социальными группами, учитывает культурные и религиозные традиции, при личном и массовом общении, определяет приемы конструктивного взаимодействия в ситуации общения, ставит цели в своей профессиональной деятельности и решает профессиональные задачи с учётом своих ресурсных возможностей и приоритетов, выбирает эффективные стратегии и тактики личностного и профессионального развития, пользуется методикой оценки эффективности применяемых методов решения поставленных задач в сфере своей профессиональной деятельности, оценивает эффективность использования времени и других ресурсов при решении поставленных задач в избранной сфере профессиональной деятельности, проводит критическую оценку эффективности использования своего времени и других ресурсов, при решении задач, поставленных в избранной сфере профессиональной деятельности, применяет методы решения задач моделирования и проектирования автоматизированных информационных систем и систем обеспечения информационной безопасности, разрабатывает и обосновывает критерии оценки эффективности проектируемой системы обеспечения информационной безопасности, разрабатывает актуальную модель угроз для автоматизированных информационных систем и учитывает её положения при формировании требований технического задания на проектируемую систему обеспечения информационной безопасности, проводит разработку и обосновывает критерии оценки эффективности проектируемой системы обеспечения информационной безопасности, оценивает эффективность решений и анализирует показатели деятельности, определяет направления развития и проблем компьютерного моделирования сложных систем, разработке и исследовании системы защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасности, реализовывает типовые задачи средствами автоматизированного и ручного функционального тестирования, учитывает направления развития технологий проектирования информационных, автоматизированных и автоматических систем, управляет коллективом исполнителей и принимает управленческие решения, соблюдает правила построения оптимальной политики безопасности в соответствии с требованиями уровня безопасности, определяет стоимость и сроки реализации проекта, работает с нормативными правовыми актами в области информационной безопасности с технической и эксплуатационной документацией, оценивает различные инструменты в области проектирования и управления информационной безопасностью, соблюдает основы отечественных и зарубежных стандартов в области сертификации и аттестации объектов информатизации, учитывает основные угрозы безопасности информации и модели нарушителя в информационных системах, разрабатывает политики безопасности различных уровней, рассчитывает и разрабатывает положения о применимости механизмов контроля в контексте управления рисками информационной безопасности, соблюдает правила построения оптимальной политики безопасности в соответствии с требованиями уровня безопасности, определяет стоимость и сроки реализации проекта, работает с нормативными правовыми актами в области информационной безопасности с технической и эксплуатационной документацией, оценивает различные инструменты в области проектирования и управления информационной безопасностью, соблюдает основы отечественных и зарубежных стандартов в области сертификации и аттестации объектов информатизации, учитывает основные угрозы безопасности информации и модели нарушителя в информационных системах, разрабатывает политики безопасности различных уровней, рассчитывает и разрабатывает положения о применимости механизмов контроля в контексте управления рисками информационной безопасности, формулирует научную проблему, анализирует гипотезы, проводит выбор предмета, объекта, целей, задач исследования, создаёт эскизный, технический, рабочий проект, применяет технологии поиска, изучения, обобщения и систематизации научной информации, определяет комплекс мер для обеспечения безопасности информационных систем, составляет аналитические обзоры по вопросам обеспечения информационной безопасности систем, использует методы и средства анализа защищенности информационных систем, программные и аппаратные средства персонального компьютера для поиска и обработки информации, формулирует научную проблему, анализирует гипотезы, применяет методику создания

технического задания и технического проекта при организации НИОКР, определяет порядок организации процесса исследования, методы построения оптимальных планов для научных экспериментов, оформляет научные публикации в соответствии с шаблоном IEEE, требованиями научных конференций, разрабатывает техническую документацию в соответствии с требованиями Единой системы конструкторской документации и Единой системы программной документации, анализирует получаемые результаты и формулирует выводы, выбирает и обосновывает критерии оценки защищенности открытых информационных систем, готовит научные доклады и статьи.

Государственный экзамен проводится с соблюдением объективности и взаимного уважения студента, и экзаменатора. Основными принципами процедуры оценивания ответа студента членами Государственной аттестационной комиссии на государственном экзамене являются: профессионализм, предметность, независимость, объективность, непредвзятость, беспристрастность, доброжелательность.

Основной задачей государственной аттестационной комиссии является определение соответствия подготовки выпускников квалификационным требованиям федерального государственного образовательного стандарта высшего профессионального образования по направлению 10.04.01 «Информационная безопасность».

При оценивании ответов студентов экзаменаторы руководствуются системой критериев:

Содержательное соответствие – соответствие содержания ответа поставленным на экзамене вопросам.

Методологическая обоснованность – построение ответа в соответствии с уровнями методологии научного знания, умение представить современное состояние развития информационных технологий, зарубежные научные подходы, теории и результаты исследований в критическом сравнении с достижениями отечественной науки.

Научный анализ – критический научный анализ излагаемых концепций, аргументированный конкретными результатами.

Научный синтез – рассмотрение теоретических подходов, отдельных концепций и исследований в контексте научного знания в целом, демонстрация понимания связи между отдельными элементами целостного научного знания, обобщение и систематизация научной информации при решении проблемы.

Системность – четкое выделение понятий, существенных элементов теорий или концепций, их характеристика, описание связей между ними, представление материала как цельной системы знаний.

Логичность – последовательное, непротиворечивое, четко структурированное изложение материала с выделением основополагающих и второстепенных положений ясность изложения материала.

Понятийно-терминологическая обоснованность – использование при изложении материала адекватных научных профессиональных информационных и математических терминов и понятий, раскрытие их полного содержания, соответствующего современному уровню развития информационных технологий.

Проявление индивидуальной и профессиональной культуры.

При оценивании ответов студентов экзаменаторы отмечают достоинства ответов при их наличии, их соответствие указанным критериям, выделяют следующие типы несоответствий в виде неточностей или ошибок (при их наличии):

Неточность:

При изложении теоретического материала - незначительная погрешность, не искажающая смысла излагаемого материала, отсутствие в ответе ссылок на некоторых авторов конкретных теорий и исследований, изложение теорий или исследований без указания времени проведения исследований или создания концепций, имеющих отношение к вопросу.

При использовании терминологии – неполное представление о содержании понятий, использование жаргонных слов вместо научной терминологии при правильном изложении теоретического и эмпирического материала.

При изложении теоретических вопросов - слабая аргументированность, недостаточное подтверждение теоретических положений известными фактами и феноменами.

Ошибка:

При изложении теоретического материала - грубые искажения в описании научных теорий и концепций, неадекватное раскрытие содержания излагаемого вопроса пропуски важных смысловых элементов материала отсутствие в тексте или устном ответе описаний одного или более из основных теоретических подходов или ключевых компонентов излагаемой теории, перестановки и смещения в хронологии фактического или логического концептуального изложения материала.

При изложении эмпирического и (или) экспериментального материала - неадекватное использование или незнание методов, методик, тестов, измерительных параметров и процедур проведения исследований, существенных характеристик выборки, неадекватная интерпретация полученных основных результатов и выводов.

При использовании терминологии - неумение оперировать категориальным аппаратом, незнание основных научных информационных и математических терминов и понятий.

Форма оценивания членами ГЭК результатов освоения образовательной программы (уровня сформированности компетенций) выпускника при сдаче государственного экзамена по направлению подготовки - 10.04.01 «Информационная безопасность» квалификация магистр

№ п/п	Критерии оценки	отлично	хорошо	удовлетворительно	неудовлетворительно
1.	Полнота раскрытия вопросов экзаменационного билета (указать УК или ОПК)				
2.	Аргументированность ответа студента (указать УК или ОПК)				
3.	способность анализировать и сравнивать различные подходы к решению поставленной проблемы (указать УК или ОПК)				
4.	готовность студента отвечать на дополнительные вопросы по существу экзаменационного билета (указать УК или ОПК)				
5.	Навыки защиты собственных научных идей, предложений и рекомендаций (указать УК или ОПК)				
6.	Общий уровень культуры общения указать УК или ОПК)				
7.	Готовность к практической деятельности в условиях рыночной экономики, изменения при необходимости направления профессиональной деятельности в рамках предметной области знаний и практических навыков (указать УК или ОПК)				

Распределение оценок членов ГЭК по компетенциям для определения общего уровня сформированности требуемых компетенций при сдаче государственного экзамена

№ п/п	Члены ГЭК	Компетенции													
		УК–1				УК–2	УК–3	УК–4	УК–5	УК–6	ОП К-1	ОП К-2	ОП К-3	ОП К-4	ОП К-5
		Оценка по критерию													
		1		1 1	среднее										
1.															
2.															
3.															
4.															
5.															
Среднее значение по компетенции															

Перечень компетенций, знаний, умений, владений, уровень усвоения которых должен быть проверен на защите выпускной квалификационной работы

Цели и задачи проведения защиты ВКР в соответствии с требованиями ФГОС ВПО по направлению 10.04.01 «Информационная безопасность» состоят в выявлении уровня теоретической подготовки специалиста и степени его подготовленности к профессиональной деятельности в области информационной безопасности.

Выпускник магистратуры по направлению подготовки «Информационная безопасность» должен:

знать: новые методы исследования в профессиональной деятельности, направления развития информационных (телекоммуникационных) технологий, методы разработки систем, комплексов, средств и технологий обеспечения информационной безопасности, способы проведения обоснования состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов, программы и методики испытаний средств и систем обеспечения информационной безопасности, методы анализа фундаментальных и прикладных проблем информационной безопасности в условиях становления, методику сбора, обработки, анализа и систематизации научно-технической информации по теме исследования, выбора методов, методы проведения экспериментальных исследований защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента, методы обработки результатов экспериментальных исследований, методику проведения аудита информационной безопасности информационных систем и объектов информатизации, методики проведения занятий по избранным дисциплинам предметной области данного направления и разработки методических материалов, используемых в образовательной деятельности, методики управления коллективом исполнителей и принятия управленческих решений, методы организации управления информационной безопасностью, нормативные акты и нормативные методические документы ФСБ России, ФСТЭК России, порядок выполнения работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности, порядок разработки проектов, организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности,

уметь: применять новые методы исследования в профессиональной деятельности, анализировать направления развития информационных (телекоммуникационных) технологий, применять методы разработки систем, комплексов, средств и технологий обеспечения информационной безопасности, проводить обоснования состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов, применять программы и методики испытаний средств и систем обеспечения информационной безопасности, методы анализа фундаментальных и прикладных проблем информационной безопасности в условиях становления, методику сбора, обработки, анализа и систематизации научно-технической информации по теме исследования, выбирать методики проведения экспериментальных исследований защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента, применять методы обработки результатов экспериментальных исследований, методику проведения аудита информационной безопасности информационных систем и объектов информатизации, методики проведения занятий по избранным дисциплинам

предметной области данного направления и разработки методических материалов, используемых в образовательной деятельности, методики управления коллективом исполнителей и принятия управленческих решений, методы организации управления информационной безопасностью, нормативные акты и нормативные методические документы ФСБ России, ФСТЭК России, уметь выполнять работы по вводу в эксплуатацию систем и средств обеспечения информационной безопасности, разрабатывать проекты, организационно-распорядительные документы, бизнес-планы в сфере профессиональной деятельности,

владеть: способностью к абстрактному мышлению, анализу, синтезу, самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения, способностью к коммуникации в устной и письменной формах на государственном и одном из иностранных языков для решения задач профессиональной деятельности, к самостоятельному обучению и применению новых методов исследования профессиональной деятельности, способностью анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность, разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности, проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов, разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности, анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления, осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методов, проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента, обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи, проводить аудит информационной безопасности информационных систем и объектов информатизации, проводить аттестацию объектов информатизации по требованиям безопасности информации, проводить занятия по избранным дисциплинам предметной области данного направления и разрабатывать методические материалы, используемые в образовательной деятельности, организовать выполнение работ, управлять коллективом исполнителей и принимать управленческие решения, организовать управление информационной безопасностью, организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России, организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности, способностью разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной.

Форма оценивания членами ГЭК результатов освоения образовательной программы (уровня сформированности компетенций) при защите выпускной квалификационной работы) по направлению подготовки - 10.04.01 «Информационная безопасность» квалификация магистр

№ п/п	Критерии оценки	отлично	хорошо	удовлетворительно	неудовлетворительно
1.	Уровень теоретической и научно–исследовательской проработки проблемы (указать ПК)				
2.	Качество анализа проблемы (указать ПК)				
3.	Полнота и проблемность вносимых предложений по рассматриваемой проблеме (указать ПК)				
4.	Уровень апробации работы и публикаций (указать ПК)				
5.	Объем экспериментальных исследований и степень внедрения в производство (указать ПК)				
6.	Самостоятельность разработки (указать ПК)				
7.	Степень владения современными программными продуктами и компьютерными технологиями (указать ПК)				
8.	Навыки публичной дискуссии, защиты собственных научных идей, предложений и рекомендаций (указать ПК)				
9.	Качество презентации результатов работы(указать ПК)				
10.	Общий уровень культуры общения с аудиторией(указать ПК)				
11.	Готовность к практической деятельности в условиях рыночной экономики, изменения при необходимости направления профессиональной деятельности в рамках предметной области знаний и практических навыков (указать ПК)				

Распределение оценок членов ГЭК по компетенциям для определения общего уровня сформированности требуемых компетенций при защите выпускной квалификационной работы

№ п/п	Члены ГЭК	Компетенции						
		ПК-1				ПК-2	ПК-3	ПК-4
		1		7	среднее			
1.								
2.								
3.								
4.								
5.								
Среднее значение по компетенции								

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
Зав. кафедрой организации и
технологии защиты информации
_____ В.И. Петренко
«_____» _____ 2026 г.

График выполнения выпускной квалификационной работы

1. Направление подготовки 10.04.01 «Информационная безопасность»
2. Направленность Комплексная защита объектов информатизации

Этапы или разделы работы	Сроки выполнения
1.Выдача задания	
2.Начало проектирования	
2.Разделы ВКР	
2.1 Раздел _____	
2.2.Раздел _____	
2.3. Раздел _____	
3.Предзащита	
4.Рецензирование	
5.Сдача ВКР на кафедру	
6. Защита в ГЭК	

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное
образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

Декан факультета математики и
компьютерных наук имени
профессора Н.И.Червякова
Т. А. Грובה
«___» _____ 2026 г.

ЛИСТ ИЗМЕНЕНИЙ

в учебно-методическом комплексе ГИА
по направлению подготовки 10.04.01 «Информационная безопасность»
на 2026 учебный год

№ п/п	Элемент УМК	Перечень вносимых изменений

СОГЛАСОВАНО:

Представитель работодателя
Директор ООО «Инфоком С»
_____ Н.Г. Демурчев

РАЗРАБОТАНО:

Доцент кафедры организации и технологии
защиты информации
Бисюков Виктор Михайлович

Рассмотрено УМК факультета математики и
компьютерных наук имени профессора
Н.И.Червякова
Протокол №___ от «___» _____ 2026 г.