

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Казанский (Приволжский) федеральный университет»
Институт физики



УТВЕРЖДАЮ

Проректор по образовательной деятельности КФУ

Е.А. Турилова

17 февраля 2023 г.

подписано электронно-цифровой подписью

Программа государственной итоговой аттестации
Б3.01(Д) Подготовка к процедуре защиты и защита выпускной квалификационной работы

Направление подготовки / специальность: 10.04.01 Информационная безопасность

Направленность (профиль) подготовки Информационная безопасность автоматизированных систем

Квалификация выпускника: магистр

Форма обучения: очное

Язык обучения: русский

Год начала обучения по образовательной программе: 2023

Содержание

1. Общие положения
2. Цели и задачи государственной итоговой аттестации
3. Структура государственной итоговой аттестации

4. Требования к профессиональной подготовленности выпускника

ПРОГРАММА ГОСУДАРСТВЕННОГО АТТЕСТАЦИОННОГО ИСПЫТАНИЯ.

ПОДГОТОВКА К ПРОЦЕДУРЕ ЗАЩИТЫ И ЗАЩИТА ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ

1. Компетенции, освоение которых проверяется выпускной квалификационной работой
2. Объем выполнения и защиты выпускной квалификационной работы в зачетных единицах и часах
3. Цели, принципы и этапы подготовки к процедуре защиты и защиты выпускной квалификационной работы
- 3.1. Цели и принципы подготовки к процедуре защиты и защиты выпускной квалификационной работы
- 3.2. Этапы и сроки выполнения выпускной квалификационной работы
4. Темы выпускных квалификационных работ
5. Фонд оценочных средств по подготовке к процедуре защиты и защите выпускной квалификационной ра-

боты

6. Методические рекомендации по подготовке к процедуре защиты и защите выпускной квалификационной работы

7. Список литературы, необходимой для подготовки к процедуре защиты и защиты выпускной квалификационной работы

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для подготовки к процедуре защиты и защиты выпускной квалификационной работы

9. Перечень информационных технологий, используемых для подготовки к процедуре защиты и защиты выпускной квалификационной работы, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

10. Описание материально-технического обеспечения, необходимого для подготовки к процедуре защиты и защиты выпускной квалификационной работы

11. Особенности подготовки к процедуре защиты и защиты выпускной квалификационной работы для обучающихся инвалидов и лиц с ограниченными возможностями здоровья

ПРИЛОЖЕНИЯ к программе государственного аттестационного испытания «Подготовка к процедуре защиты и защита выпускной квалификационной работы»

Приложение № 1. Фонд оценочных средств

Приложение №2. Оценочный лист по подготовке к процедуре защиты и защите выпускной квалификационной работы для очной и очно-заочной форм обучения

Приложение №3. Список литературы, необходимой для подготовки к процедуре защиты и защиты выпускной квалификационной работы

Приложение №4. Перечень информационных технологий, используемых для подготовки к процедуре защиты и защиты выпускной квалификационной работы, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Приложение №5. Макет отзыва научного руководителя выпускной квалификационной работы.

Приложение №6. Макет рецензии на выпускную квалификационную работу.

1. Общие положения

Настоящая программа разработана в целях организации и проведения государственной итоговой аттестации по основной профессиональной образовательной программе высшего образования по направлению подготовки / специальности 10.04.01 Информационная безопасность (Информационная безопасность автоматизированных систем) (далее – ОПОП ВО).

2. Цели и задачи государственной итоговой аттестации

В соответствии с Законом «Об образовании в Российской Федерации», выпускники, завершающие обучение по ОПОП ВО, проходят государственную итоговую аттестацию. Государственная итоговая аттестация (далее – ГИА) предназначена для определения уровня теоретической и практической подготовленности выпускника к выполнению профессиональных задач, установленных федеральным государственным образовательным стандартом высшего образования (далее – ФГОС ВО).

ГИА выпускников осуществляется после освоения ОПОП ВО в полном объеме.

Целью ГИА является установление уровня подготовленности обучающихся, осваивающих ОПОП ВО, к выполнению профессиональных задач и соответствия их подготовки требованиям ФГОС ВО.

3. Структура государственной итоговой аттестации

Государственная итоговая аттестация по данной ОПОП ВО включает следующие государственные аттестационные испытания:

- подготовка к процедуре защиты и защита выпускной квалификационной работы.

4. Требования к профессиональной подготовленности выпускника

Результаты освоения ОПОП ВО определяются приобретаемыми выпускником компетенциями, т.е. его способностью применять знания, умения и навыки в соответствии с задачами профессиональной деятельности.

В результате освоения ОПОП ВО согласно ФГОС ВО выпускник должен обладать следующими компетенциями:

Шифр компетенции	Расшифровка проверяемой компетенции
<i>Универсальные компетенции (УК)</i>	
УК-1	Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий
УК-2	Способен управлять проектом на всех этапах его жизненного цикла
УК-3	Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели
УК-4	Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия
УК-5	Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия
УК-6	Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки
<i>Общепрофессиональные компетенции (ОПК)</i>	
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
<i>Профессиональные компетенции (ПК)</i>	
ПК-1	Способность анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты
ПК-2	Способность проводить аудит информационной безопасности информационных систем и объектов информатизации
ПК-3	Способность проводить аттестацию объектов информатизации по требованиям безопасности информации
ПК-4	Способность создания педагогических условий для развития группы обучающихся по программам ВО, организационно-методическое, преподавание для программ бакалавриата, ориентированным на соответствующий уровень квалификации
ПК-5	Способность организовать управление информационной безопасностью
ПК-6	Способен обобщать и критически оценивать опыт и результаты научных исследований в области информационной безопасности

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
"Казанский (Приволжский) федеральный университет"
Институт физики



УТВЕРЖДАЮ

Проректор по образовательной деятельности КФУ
Е.А. Турилова

17 февраля 2023 г.

подписано электронно-цифровой подписью

Программа государственной итоговой аттестации
Б3.01(Д) Подготовка к процедуре защиты и защита выпускной квалификационной работы

Направление подготовки / специальность: 10.04.01 Информационная безопасность
Направленность (профиль) подготовки Информационная безопасность автоматизированных систем
Квалификация выпускника: магистр
Форма обучения: очное
Язык обучения: русский
Год начала обучения по образовательной программе: 2023

1. Компетенции, освоение которых проверяется выпускной квалификационной работой

Выпускник должен обладать следующими компетенциями:

Шифр компетенции	Расшифровка проверяемой компетенции
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 способности 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	Способность анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты
ПК-2	Способность проводить аудит информационной безопасности информационных систем и объектов информатизации
ПК-3	Способность проводить аттестацию объектов информатизации по требованиям безопасности информации
ПК-4	Способность создания педагогических условий для развития группы обучающихся по программам ВО, организационно-методическое сопровождение, преподавание для программ бакалавриата, ориентированным на соответствующий уровень квалификации
ПК-5	Способность организовать управление информационной безопасностью
ПК-6	Способен обобщать и критически оценивать опыт и результаты научных исследований в области информационной безопасности

2. Объем выполнения и защиты выпускной квалификационной работы в зачетных единицах и часах

Общая трудоемкость составляет 9 зачетных единиц на 324 часа.

Из них:

6 часов отводится на КСР; реализуются в форме консультационной работы преподавателя по вопросам организации и проведения государственной итоговой аттестации;

309 часов отводится на самостоятельную работу;

9 часов отводится на контроль.

3. Цели, принципы и этапы подготовки к процедуре защиты и защиты выпускной квалификационной работы

3.1. Цели и принципы подготовки к процедуре защиты и защиты выпускной квалификационной работы

Выпускная квалификационная работа (далее – ВКР) представляет собой выполненную обучающимся (несколькими обучающимися совместно) работу, демонстрирующую уровень подготовленности выпускника к самостоятельной профессиональной деятельности.

ВКР является обязательной формой государственной итоговой аттестации, самостоятельно выполняемой обучающимися на завершающем этапе освоения ОПОП ВО. В ВКР на основе профессионально-ориентированной теоретической подготовки решаются конкретные теоретические и практические задачи, предусмотренные соответствующей ступенью высшего образования.

Цель представления ВКР - демонстрация степени готовности выпускника к осуществлению соответствующих видов профессиональной деятельности.

Задачами ВКР являются: расширение, систематизация и закрепление теоретических и практических знаний и применение их в профессиональной деятельности, совершенствование навыков ведения самостоятельной творческой работы, способности четко, ясно и логично излагать в письменной форме свои мысли по избранной тематике.

Для подготовки ВКР обучающемуся назначается руководитель (из числа работников КФУ) и, при необходимости, консультанты. Руководитель ВКР:

- оказывает помощь обучающемуся в выборе темы и разработке календарного графика работы;
- помогает ориентироваться в литературе по теме работы;
- оказывает помощь в определении направления исследования, подборе понятийного и методологического аппарата;
- помогает в выборе методов и методик исследования, обработке и анализе полученных результатов;
- проверяет выполнение этапов работы;
- составляет письменный отзыв о работе обучающегося;
- оказывает помощь в подготовке к защите ВКР.

3.2. Этапы и сроки выполнения выпускной квалификационной работы

Начальным этапом выполнения выпускной квалификационной работы является выбор темы. Своевременный и правильный выбор темы определяет успех всей последующей работы обучающегося. Прежде всего, обучающемуся необходимо ознакомиться с примерной тематикой выпускных квалификационных работ.

Тематическое решение исследовательских задач выпускной квалификационной работы необходимо ориентировать на разработку конкретных проблем, имеющих научно-практическое значение. При разработке перечня рекомендуемых тем выпускных квалификационных работ кафедры исходит из того, что эти темы должны:

- соответствовать компетенциям, получаемым обучающимися;
- включать основные направления, которыми обучающемуся предстоит заниматься в своей будущей профессиональной деятельности.

Перечень тем, предлагаемых кафедрой вниманию обучающихся, не является исчерпывающим. Обучающийся может предложить свою тему с соответствующим обоснованием необходимости и целесообразности ее разработки и осуществлять выполнение выпускной квалификационной работы, получив разрешение заведующего выпускающей кафедрой. При этом самостоятельно выбранная тема должна отвечать направленности (профилю) подготовки обучающегося с учетом его научных интересов, стремлений и наклонностей.

Работа с научным руководителем должна присутствовать в течение всего периода написания выпускной квалификационной работы. Она включает в себя следующие виды работ:

- обсуждение темы выпускной квалификационной работы,
- определение целей и задач исследования или разработки,
- способов и методов, с помощью которых можно их достичь,
- анализ и выбор необходимого программного обеспечения, необходимого мультимедийного и сетевого оборудования, конкретная детализация этапов работы.

Научный руководитель занимается не только постановкой задачи и контролем его исполнения. Рекомендуется планомерно в течение всего периода написания работы консультироваться с научным руководителем. Эти консультации должны включать как отчеты о проделанной работе, так и разбор сомнений, проблем студента, получение рекомендаций по выполнению дальнейших этапов работы, получение советов по изучению подходящей учебной и научной литературы и других источников и пр.

Поиск и сбор информации для исследований и разработок является вторым этапом. Особенно интересными являются те темы выпускных квалификационных работ, которые не имеют очевидного для студента решения. Именно такие темы будут способствовать формированию у студентов необходимых профессиональных качеств и навыков, поскольку потребуют развития и большего объема разноплановой работы. В случае магистерских диссертаций выбор темы имеет особенно важное значение, так как тема должна быть научно-исследовательской, способствующей формированию компетенций научной работы студента. В случае выбора студентом таких тем необходимым этапом работы становится сбор теоретического и прикладного материала, необходимого для написания выпускной квалификационной работы.

В любом случае начальным этапом непосредственно самостоятельной работы студента после обсуждения темы с руководителем является исследование полученной задачи, выявление ее основных свойств, методов решения, анализ предметной области, выбор используемых программных и аппаратных средств и информационные технологии, используемых в работе. Конечно, руководитель даст ответы на некоторые из этих вопросов. Однако в большинстве случаев этого будет недостаточно. Студент должен сам уметь находить необходимую для выпускной квалификационной работы информацию. Рекомендуемое время окончания предварительного сбора и исследований – до 20 февраля.

Основной этап выполнения работы сильно зависит от выбранной темы исследования и разработки и имеет большое количество форм. Так, в случае теоретических разработок, этот этап связан с анализом и систематизацией собранного научного материала, выявлением и анализом основных тенденций, закономерностей в области информационной безопасности, формулировкой и доказательством (обоснованием) теоретических положений, эмпири-

ческим исследованием. Эмпирическое исследование зачастую связано с созданием программного продукта, реализующего предлагаемую методику, и проведение с его помощью вычислительного эксперимента и последующего его анализа. В задачах информационной безопасности, помимо анализа и систематизации собранного материала, важное значение имеют исследование и анализ предметной области разработки, анализ существующих аналогов разработки, разработка проекта программного обеспечения, выбор инструментальных средств разработки и аргументация данного выбора, определение и разработка алгоритмов обработки информации, используемой в программе, исправление замечаний, высказанных научным руководителем. Рекомендуемое время окончания этапа разработки – 30 апреля.

Этап верификации и тестирования, проведения эксперимента, является одним из важных этапов работы, поскольку позволяет выявить результаты исследуемых или применяемых алгоритмов и оценить их эффективность. Рекомендуемый срок окончания этапа – 15 мая.

Оформление работы в виде пояснительной записки. Обычно пояснительной запиской считается текст, включающий в себя полное описание задачи и хода ее решения, представление и анализ полученных результатов, анализ и формулировку выводов от сделанного исследования или разработки. В зависимости от темы работы рекомендуется делить текст на три главы, которые отражают теоретические аспекты решаемой задачи, описание способа решения, практическая глава, описывающая принципы функционирования созданного программного обеспечения или анализ результатов экспериментов рассматриваемых методик.

Последний этап связан с подготовкой к защите выпускной квалификационной работы, который проверяется в ходе предзащиты, на которой студент представляет презентацию своей работы и текст ВКР. Предзащита призвана не столько проверить готовность работы, сколько провести репетицию защиты, дать студентам ценные рекомендации по тексту работы и по акцентам, сделанным в презентации.

Готовый текст ВКР распечатывается, переплетается и передается на выпускающую кафедру. Руководитель ВКР пишет отзыв на ВКР. Отзыв составляется по форме, указанной в Приложении 5 к настоящей программе. В отзыве отражается мнение руководителя о работе обучающегося над ВКР в течение учебного года, об уровне текста ВКР, о соответствии ВКР предъявляемым требованиям. ВКР подлежит рецензированию. Рецензентом выступает преподаватель КФУ или сотрудник иной организации, являющийся специалистом в предметной области ВКР. Рецензия оформляется по форме, приведенной в Приложении 6 к настоящей программе. Отзыв руководителя и рецензия вместе с текстом ВКР представляются государственной экзаменационной комиссии во время защиты ВКР.

ВКР подлежит защите в виде выступления обучающегося перед государственной экзаменационной комиссией. После выступления члены комиссии задают обучающемуся вопросы, на которые обучающийся отвечает. Озвучиваются отзыв руководителя и рецензия. Обучающемуся предоставляется возможность ответить на замечания, содержащиеся в отзыве руководителя и рецензии (при наличии). Государственная экзаменационная комиссия принимает решение о выставлении оценки на закрытом заседании большинством голосов. При равном количестве голосов голос председателя комиссии (при отсутствии председателя – его заместителя) является решающим.

4. Темы выпускных квалификационных работ

Примерный список тем ВКР ежегодно разрабатывается на соответствующей кафедре и доводится до сведения обучающихся не позднее, чем за 6 месяцев до даты начала ГИА. Обучающийся имеет право предложить свою тему ВКР с необходимым обоснованием целесообразности ее разработки.

Примерный перечень тем ВКР представлен в фонде оценочных средств.

5. Фонд оценочных средств по подготовке к процедуре защиты и защите выпускной квалификационной работы

Фонд оценочных средств по подготовке к процедуре защиты и защите выпускной квалификационной работы включает в себя следующие компоненты:

- соответствие компетенций проверяемым результатам обучения;
- критерии оценивания сформированности компетенций;
- механизм формирования оценки за выпускную квалификационную работу;
- описание процедуры оценивания текста выпускной квалификационной работы, защиты выпускной квалификационной работы, результатов промежуточной аттестации и портфолио (при необходимости);
- требования к тексту выпускной квалификационной работы, к защите выпускной квалификационной работы к результатам промежуточной аттестации и портфолио (при необходимости);
- критерии оценивания выпускной квалификационной работы;
- примерные темы выпускных квалификационных работ.

Фонд оценочных средств по подготовке к процедуре защиты и защите ВКР представлен в Приложении 1 к данной программе.

Макет оценочного листа подготовки к процедуре защиты и защиты ВКР для обучающихся очной и очно-заочной форм обучения представлен в Приложении 2 к данной программе.

6. Методические рекомендации по подготовке к процедуре защиты и защите выпускной квалификационной работы

Работа над выпускной квалификационной работой начинается с определения точной ее темы в начале обучения на 2 курсе. В этот период особенно важно часто встречаться с научным руководителем, осуществлять поиск информации по теме и по смежным с ней, получить максимально широкое представление о текущем состоянии проблемы. В ряде случаев это время может быть посвящено изучению технологий разработки программного продукта, предусмотренного выпускной квалификационной работой.

В период зимних каникул рекомендуется сформулировать и согласовать с руководителем поэтапный план работы, используемые методы, технологии, четко описать ожидаемый результат. Данные положения следует оформить в виде задания на выпускную квалификационную работу.

Непосредственное выполнение выпускной квалификационной работы частично будет совпадать по времени с основным образовательным процессом. Но, тем не менее, особенно важно именно в этот срок выполнить большую часть работы. Рекомендуется в этот период выделять для выполнения выпускной квалификационной работы не менее 3-4 часов 2 раза в неделю. Тогда прогресс выполнения будет всегда ощутим и студенту не потребуется вспоминать о том, чем он завершил работу несколько недель назад.

Рекомендуется активно общаться с руководителем работы, демонстрировать промежуточные результаты, получать консультации по вопросам, которые оказались сложными. В случае регулярных консультаций будет возможно оперативно обнаруживать ошибки и недочеты и вовремя их исправлять.

Отдельное внимание необходимо уделить написанию текста выпускной квалификационной работы. Текст работы должен содержать четкое описание как теоретических положений, лежащих в основе работы, так и описание практической части, которая в зависимости от темы может содержать подробное описание разработанного программного обеспечения и его функциональных возможностей или результатов экспериментов, которые были проведены с его помощью. Рекомендуется внимательно следовать требованиям оформления работы, поскольку это позволит создать целостное и системное впечатление от работы выпускника.

Выступление на защите также требует большого внимания при подготовке к нему. Важно обязательно выступить на предзащите работы, поскольку на ней можно получить ценные советы и рекомендации, как лучше представить результаты своей работы, как уложиться в отведенное время, как лучше сделать презентацию, как акценты являются наиболее выигрышными в представлении работы.

Общие рекомендации по оформлению презентации, следующие:

- должно быть не более 15 информационных слайдов;
- начинать презентацию следует с титульного листа;
- второй слайд должен быть посвящен описанию цели и задачам работы;
- следует использовать минимальное количество текста на слайде, он должен быть тезисным;
- удобным для восприятия является графический материал, поэтому большинство слайдов должны содержать схемы, графики, экранные формы и прочие изображения, демонстрирующие результаты работы;
- желательно использовать контрастную цветовую гамму.

При ответах на вопросы членов государственной экзаменационной комиссии следует внимательно слушать вопрос, можно апеллировать при ответе к слайдам презентации или указанию на примерное место ответа в тексте выпускной квалификационной работы. Очень важно, чтобы ответы на вопросы скорее напоминали беседу, аргументированную дискуссию.

7. Список литературы, необходимой для подготовки к процедуре защиты и защиты выпускной квалификационной работы

Выполнение ВКР предполагает изучение учебной литературы. Литература может быть доступна обучающимся в одном из двух вариантов (либо в обоих из них):

- в электронном виде – через электронные библиотечные системы на основании заключенных КФУ договоров с правообладателями;
- в печатном виде – в Научной библиотеке им. Н.И. Лобачевского. Обучающиеся получают учебную литературу на абонементе по читательским билетам в соответствии с правилами пользования Научной библиотекой.

Электронные издания доступны дистанционно из любой точки при введении обучающимся своего логина и пароля от личного кабинета в системе «Электронный университет». При использовании печатных изданий библиотечный фонд должен быть укомплектован ими из расчета не менее 0,5 экземпляра каждого из изданий основной литературы и не менее 0,25 экземпляра дополнительной литературы на каждого обучающегося из числа лиц, одновременно осуществляющих подготовку к сдаче государственного экзамена по данной ОПОП ВО.

Список литературы, необходимой для подготовки к процедуре защиты и защиты ВКР, представлен в Приложении 3 к данной программе.

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для подготовки к процедуре защиты и защиты выпускной квалификационной работы

Наименование Интернет-ресурса	URL
Интернет-портал образовательных ресурсов по ИТ	http://www.intuit.ru
Интернет-портал с научными ресурсами по математическим наукам	http://www.mathnet.ru
Научная электронная библиотека	https://elibrary.ru/defaultx.asp

Научная электронная библиотека КиберЛенинка	https://cyberleninka.ru/
Образовательная платформа Stepik	https://welcome.stepik.org/ru
ЭБС Знаниум	http://znanium.com
ЭБС Лань	http://e.lanbook.com
Информационный бюллетень "Jet Info" с тематическим разделом по информационной безопасности	http://www.jetinfo.ru
Сервер компании НИП "Информзащита"	http://www.infosec.ru

9. Перечень информационных технологий, используемых для подготовки к процедуре защиты и защиты выпускной квалификационной работы, включая перечень программного обеспечения и информационных справочных систем

Перечень информационных технологий, используемых для подготовки к защите и защите ВКР, включая перечень программного обеспечения и информационных справочных систем (при необходимости), представлен в Приложении 4 к данной программе.

10. Описание материально-технического обеспечения, необходимого для подготовки к процедуре защиты и защиты выпускной квалификационной работы

Материально-техническое обеспечение подготовки к процедуре защиты и защиты ВКР включает в себя следующие компоненты:

- помещения для самостоятельной работы обучающихся по выполнению ВКР и подготовке к защите, укомплектованные специализированной мебелью (столы и стулья) и оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду КФУ;
- учебные аудитории для консультаций, укомплектованные специализированной мебелью (столы и стулья);
- аудитории для заседания государственной экзаменационной комиссии и для заседания апелляционной комиссии, укомплектованные специализированной мебелью (столы и стулья);
- проектор и экран для презентации при защите ВКР;

11. Особенности подготовки к процедуре защиты и защиты выпускной квалификационной работы для обучающихся инвалидов и лиц с ограниченными возможностями здоровья

При необходимости в образовательном процессе применяются следующие методы и технологии, облегчающие подготовку к защите и защите выпускной квалификационной работы лицам с ОВЗ и инвалидам:

- создание текстовой версии любого нетекстового контента для его возможного преобразования в альтернативные формы, удобные для различных пользователей;
- создание контента, который можно представить в различных видах без потери данных или структуры, предусмотреть возможность масштабирования текста и изображений без потери качества, предусмотреть доступность управления контентом с клавиатуры;
- создание возможностей для обучающихся воспринимать одну и ту же информацию из разных источников - например, так, чтобы лица с нарушениями слуха получали информацию визуально, с нарушениями зрения - аудиально; применение программных средств, обеспечивающих возможность выполнения и защиты выпускной квалификационной работы, за счёт альтернативных способов, в том числе виртуальных лабораторий и симуляционных технологий;
- применение дистанционных образовательных технологий для организации консультаций;
- применение дистанционных образовательных технологий для организации защиты выпускной квалификационной работы для лиц с ОВЗ и инвалидов и предоставляется право выбора, с учетом индивидуальных психофизических особенностей, формы проведения итоговой аттестации (устно, письменно, с использованием технических средств и др.);
- для выступления на защите выпускной квалификационной работы лицам с ОВЗ и инвалидам могут быть предоставлены специальные технические средства, возможно привлечение ассистентов;
- увеличение продолжительности выступления лиц с ОВЗ и инвалидов при защите выпускной квалификационной работы – не более чем на 15 минут.

Приложение № 1

к программе государственного аттестационного испытания
Б3.01(Д) «Подготовка к процедуре защиты и защита выпускной квалификационной работы»

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Казанский (Приволжский) федеральный университет»
Институт физики

**Фонд оценочных средств государственного аттестационного испытания
Б3.01(Д) Подготовка к процедуре защиты и защита выпускной квалификационной работы**

Направление подготовки / специальность: 10.04.01 Информационная безопасность
Направленность (профиль) подготовки Информационная безопасность автоматизированных систем
Квалификация выпускника: магистр
Форма обучения: очное
Язык обучения: русский
Год начала обучения по образовательной программе: 2023

СОДЕРЖАНИЕ

1. СООТВЕТСТВИЕ КОМПЕТЕНЦИЙ ПРОВЕРЯЕМЫМ РЕЗУЛЬТАТАМ ОБУЧЕНИЯ

2. ИНДИКАТОРЫ ОЦЕНИВАНИЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

3. МЕХАНИЗМ ФОРМИРОВАНИЯ ОЦЕНКИ ЗА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ РАБОТУ

3.1. МЕХАНИЗМ ФОРМИРОВАНИЯ ОЦЕНКИ ДЛЯ ОБУЧАЮЩИХСЯ ОЧНОЙ И ОЧНО-ЗАОЧНОЙ ФОРМ ОБУЧЕНИЯ (С ПРИМЕНЕНИЕМ БАЛЛЬНО-РЕЙТИНГОВОЙ СИСТЕМЫ).

4. ОЦЕНОЧНЫЕ СРЕДСТВА, ПОРЯДОК ИХ ПРИМЕНЕНИЯ И КРИТЕРИИ ОЦЕНИВАНИЯ

4.1. ПРОЦЕДУРА ПРИМЕНЕНИЯ ОЦЕНОЧНОГО СРЕДСТВА

4.1.1. Процедура оценивания текста выпускной квалификационной работы

4.1.2. Процедура оценивания защиты выпускной квалификационной работы

4.1.3. Процедура оценивания результатов промежуточной аттестации и портфолио обучающегося

4.2. ТРЕБОВАНИЯ К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ

4.2.1. Требования к тексту выпускной квалификационной работы

4.2.2. Требования к защите выпускной квалификационной работы

4.2.3. Требования к результатам промежуточной аттестации и портфолио обучающегося

4.3. КРИТЕРИИ ОЦЕНИВАНИЯ ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ

4.4. ПРИМЕРНЫЕ ТЕМЫ ВЫПУСКНЫХ КВАЛИФИКАЦИОННЫХ РАБОТ

1. Соответствие компетенций проверяемым результатам обучения

Код и наименование компетенции	Индикаторы достижения компетенций	Оценочное средство
УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	ИУК-1-1. Знать принципы сбора, отбора и обобщения информации ИУК-1-2. Уметь соотносить разнородные явления и систематизировать их в рамках избранных видов профессиональной деятельности ИУК-1-3. Иметь практический опыт работы с информационными объектами и сетью Интернет, опыт научного поиска, опыт библиографического разыскания, создания научных текстов	Текст ВКР Защита ВКР
УК-2 Способен управлять проектом на всех этапах его жизненного цикла	ИУК-2.1. Знать методы управления проектами; этапы жизненного цикла проекта ИУК-2.2. Уметь разрабатывать и анализировать альтернативные варианты проектов для достижения намеченных результатов; разрабатывать проекты, определять целевые этапы и основные направления работ ИУК-2.3. Иметь практический опыт: разработки проектов в избранной профессиональной сфере; методами оценки эффективности проекта, а также потребности в ресурсах	Текст ВКР Защита ВКР
УК-3 Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	ИУК-3.1. Знать методики формирования команд; методы эффективного руководства коллективами. ИУК-3.2. Уметь разрабатывать командную стратегию; организовывать работу коллективов; управлять коллективом; разрабатывать мероприятия по личностному, образовательному и профессиональному росту. ИУК-3.3. Владеть методами организации и управления коллективом, планированием его действий.	Текст ВКР
УК-4 Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	ИУК-4.1. Знать современные коммуникативные технологии на государственном и иностранном языках; закономерности деловой устной и письменной коммуникации. ИУК-4.2. Уметь применять на практике коммуникативные технологии, методы и способы делового общения. ИУК-4.3. Владеть методикой межличностного делового общения на государственном и иностранном языках, с применением профессиональных языковых форм и средств.	Защита ВКР
УК-5 Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	ИУК-5.1. Знать сущность, разнообразие и особенности различных культур, их соотношение и взаимосвязь. ИУК-5.2. Уметь обеспечивать и поддерживать взаимопонимание между представителями различных культур и навыки общения в мире культурного многообразия. ИУК-5.3. Владеть способами анализа разногласий и конфликтов в межкультурной коммуникации и их разрешения.	Текст ВКР Защита ВКР
УК-6 Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки	ИУК-6.1. Знать основные принципы профессионального и личностного развития, исходя из этапов карьерного роста и требований рынка труда; способы совершенствования своей деятельности на основе самооценки. ИУК-6.2. Уметь решать задачи собственного профессионального и личностного развития, включая задачи изменения карьерной траектории; расставлять приоритеты. ИУК-6.3. Владеть способами управления своей познавательной деятельностью и ее совершенствования на основе самооценки и принципов образования в течение всей жизни.	Текст ВКР
ОПК-1 Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	ИОПК-1.1. Знать: основные требования к системе обеспечения информационной безопасности и уметь разрабатывать проект технического задания на ее создание. ИОПК-1.2. Уметь: уметь применять основные и профессиональные обороты русского и иностранного языка при формулировке и доказательстве научных результатов. ИОПК-1.3. Владеть: основными и профессиональными устными и письменными оборотами русского и иностранного языков при формулировке и доказательстве научных результатов	Текст ВКР
ОПК-2 Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности	ИОПК-2.1. Знать основные механизмы информационной безопасности и типовые процессы управления этими механизмами в автоматизированной системе; основные угрозы безопасности информации и модели нарушителя в информационных системах; принципы формирования политики информационной безопасности в информационных системах; методы аттестации уровня защищенности информационных систем; основные методы управления информационной безопасностью; физические основы образования технических каналов утечки информации; основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; методы концептуального проектирования технологий обеспечения информаци-	Текст ВКР Защита ВКР

	<p>онной безопасности.</p> <p>ИОПК-2.2. Уметь строить системы управления информационной безопасностью в различных условиях функционирования защищаемых автоматизированных систем; разрабатывать модели угроз и нарушителей информационной безопасности информационных систем; разрабатывать частные политики информационной безопасности информационных систем; контролировать эффективность принятых мер по реализации частных политик информационной безопасности информационных систем; оценивать информационные риски в информационных системах; разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных систем; составлять аналитические обзоры по вопросам обеспечения информационной безопасности информационных систем; применять системы компьютерной математики для решения типовых задач; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности</p> <p>ИОПК-2.3. Владеть методами и средствами выявления угроз безопасности автоматизированным системам; навыками выбора и обоснования критериев эффективности функционирования защищенных информационных систем; навыками участия в экспертизе состояния защищенности информации на объекте защиты; методами управления информационной безопасностью информационных систем; методами оценки информационных рисков; методами организации и управления деятельностью служб защиты информации на предприятии; навыками организации и обеспечения режима секретности навыками управления информационной безопасностью простых объектов</p>	
ОПК-3 Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности;	<p>ИОПК-3.1. Знать основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; методы концептуального проектирования технологий обеспечения информационной безопасности; основные нормативные правовые акты в области информационной безопасности и защиты информации; основные понятия, законы, модели и структуры обеспечения организационной безопасности на предприятии; основные понятия, законы и модели прогнозирования принятия решений;</p> <p>ИОПК-3.2. Уметь осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности; использовать нормативные правовые документы в своей профессиональной деятельности; применять основные закономерности принятия управленческих решений и управления коллективом при решении прикладных задач обеспечения информационной безопасности;</p> <p>ИОПК-3.3. Владеть навыками управления информационной безопасностью простых объектов; навыками освоения, внедрения и сопровождения документации, в том числе и в команде; навыками нахождения организационно-управленческих решений в нестандартных ситуациях на основе результатов анализа документации и потоков документов; знаниями в области правового обеспечения информационной безопасности и навыками правоприменения нормативного законодательства в данной сфере; навыками поиска нормативной и технической информации, необходимой для профессиональной деятельности, обоснования, выбора, реализации и контроля результатов работы</p>	Текст ВКР Защита ВКР
ОПК-4 Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок	<p>ИОПК-4.1. Знать основные категории и понятия информационно-аналитической работы, принципы и методы ее ведения; источники специальной информации; методы оценивания ее достоверности; виды информационных моделей и способы их построения; методы накопления специальной информации; методы подготовки специальной информации; методы выработки и принятия информационного решения; виды отчетно-информационных документов, методы их подготовки; основные математические методы исследования случайных процессов; основные теоретико-числовые методы применительно к задачам защиты информации; физические основы функционирования технических средств и систем обработки и передачи информации; физические основы образования технических каналов утечки информации; методы концептуального проектирования технологий обеспечения информационной безопасности.</p> <p>ИОПК-4.2. Уметь использовать руководящие, нормативные и методические документы по организации инфор-</p>	Текст ВКР

	<p>мационно-аналитической работы; использовать справочную и научную литературу по тематике решаемых информационных задач; оценивать специальную информацию, систематизировать ее, принимать решения о ее дальнейшем использовании; разрабатывать основные виды отчетно-информационных документов; применять средства автоматизации информационно-аналитической работы; использовать разнородные источники сведений, отчетно-информационные документы добывающих органов различных видов, в том числе на иностранном языке; применять теоретико-числовые методы для оценки криптографических свойств систем защиты информации; применять системы компьютерной математики для решения типовых задач; использовать физические эффекты для обеспечения технической защиты информации; применять на практике методы физики при исследовании технических каналов утечки информации; осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности.</p> <p>ИОПК-4.3. Владеть основными системными подходами к определению целей, задач информационно-аналитической работы и источников специальной информации; информацией о современных и перспективных системах автоматизации информационно-аналитической работы; навыками аналитического и численного решения задач математической статистики; методами проведения физического эксперимента при выявлении технических каналов утечки информации.</p>	
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.	<p>ИОПК-5.1. Знать основные классификационные признаки экспериментов; основные элементы научно-технического эксперимента; приемы выбора основных факторов эксперимента и технологию построения факторных планов, основные виды регрессионных экспериментов, основные типы оптимальных экспериментов; основные типы статистических задач и математические методы их решения; основные математические методы исследования случайных процессов; основные теоретико-числовые методы применительно к задачам защиты информации; физические основы функционирования технических средств и систем обработки и передачи информации; физические основы образования технических каналов утечки информации; основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; методы концептуального проектирования технологий обеспечения информационной безопасности..</p> <p>ИОПК-5.2. Уметь проводить классификацию экспериментов; выбирать необходимые факторы и составлять факторные планы экспериментов различного вида; строить системы базисных функций, делать точечные оценки параметров регрессионной модели; анализировать свойства оценок параметров регрессионной модели; выполнять оптимальное планирование экспериментов с использованием различных критериев; самостоятельно строить вероятностные модели применительно к практическим задачам и производить статистическую оценку адекватности полученной модели и реальных задач; применять теоретико-числовые методы для оценки криптографических свойств систем защиты информации; применять системы компьютерной математики для решения типовых задач; использовать физические эффекты для обеспечения технической защиты информации; осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности</p> <p>ИОПК-5.3. Владеть методами выбора основных факторов эксперимента; методами подбора эмпирических зависимостей для экспериментальных данных; методами оценки коэффициентов регрессионной модели эксперимента; методами построения оптимальных планов для научных экспериментов; навыками аналитического и численного решения задач; методами проведения физического эксперимента при выявлении технических каналов утечки информации</p>	Защита ВКР
ПК-1 Способность анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования	ИПК-1.1. Знать основные теоретико-числовые методы применительно к задачам защиты информации; физические основы функционирования технических средств и систем обработки и передачи информации; физические основы образования технических каналов утечки информации; основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; методы концептуально-	Текст ВКР

<p>ния, оценивать затраты и риски, формировать политику безопасности объектов защиты</p>	<p>го проектирования технологий обеспечения информационной безопасности.</p> <p>ИПК-1.2. Уметь самостоятельно строить вероятностные модели применительно к практическим задачам и производить статистическую оценку адекватности полученной модели и реальных задач; применять теоретико-числовые методы для оценки криптографических свойств систем защиты информации; применять системы компьютерной математики для решения типовых задач; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности.</p> <p>ИПК-1.3. Владеть навыками аналитического и численного решения задач математической статистики; методами проведения физического эксперимента при выявлении технических каналов утечки информации; навыками управления информационной безопасностью простых объектов.</p>	
<p>ПК-2 Способность проводить аудит информационной безопасности информационных систем и объектов информатизации</p>	<p>ИПК-2.1. Знать суть методологии и методы научного познания, методы анализа информационных процессов и систем, средства структурного анализа, математические модели информационных процессов; основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; методы концептуального проектирования технологий обеспечения информационной безопасности.</p> <p>ИПК-2.2. Уметь ставить и решать типовые задачи в области структурного анализа информационных процессов и систем, разрабатывать модели предметных областей, проводить исследования характеристик компонентов информационных процессов и информационных систем в целом; осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности.</p> <p>ИПК-2.3. Владеть методами анализа информационных процессов и систем, методами разработки математических моделей информационных процессов; навыками управления информационной безопасностью простых объектов.</p>	<p>Текст ВКР</p>
<p>ПК-3 Способность проводить аттестацию объектов информатизации по требованиям безопасности информации</p>	<p>ИПК-3.1. Знать основные принципы обеспечения информационной безопасности и защиты информации; структуру систем документационного обеспечения; основные понятия и методы в области управления службой безопасности предприятия; организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации; основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России; знать понятия и виды защищаемой информации; виды основных угроз защищаемой информации; базовые понятия о методах и средствах защиты информации; международные стандарты информационной безопасности</p> <p>ИПК-3.2. Уметь анализировать и оценивать угрозы информационной безопасности объекта; пользоваться нормативными документами по защите информации; определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности сведений, составляющих государственную и коммерческую тайну; уметь проводить процедуры аттестации, категорирования объектов информатизации; пользоваться научно-технической и справочной литературой для решения прикладных задач; осуществлять поиск информации в Интернет и выполнять аналитического исследования по определенной теме.</p> <p>ИПК-3.3. Владеть навыками анализа методов и средств передачи, хранения и обработки данных; навыками применения средств охраны от негативных воздействий; навыками оценки защищенности объектов информатизации; навыками организации охраны на объектах информатизации; навыками применения технических средств защиты информации; типовыми приемами проектирования, инструментарием для документирования проектных решений, методами прямого и обратного проектирования; навыками анализа информационной инфраструктуры информационной системы и ее безопасности; навыком пользоваться нормативными документами по противодействию технической разведке; применять действующую законодательную базу в области обеспечения ин-</p>	<p>Текст ВКР</p>

	формационной безопасности; применять нормативные правовые акты и нормативные методические документы в области обеспечения безопасности сведений, составляющих государственную и коммерческую тайну; владеть методами и средствами защиты информации, применяемыми в деятельности службы безопасности на предприятиях для обеспечения защиты сведений, составляющих государственную и коммерческую тайну	
ПК-4 Способность создания педагогических условий для развития группы обучающихся по программам ВО, организационно-методическое сопровождение, преподавание для программ бакалавриата, ориентированным на соответствующий уровень квалификации	ИПК-4.1. Знать педагогические условия для развития группы обучающихся по программам ВО, организационно-методическое сопровождение, преподавание для программ бакалавриата, ориентированным на соответствующий уровень квалификации. ИПК-4.2. Уметь создавать педагогические условия для развития группы обучающихся по программам ВО, организационно-методическое сопровождение, преподавание для программ бакалавриата, ориентированным на соответствующий уровень квалификации. ИПК-4.3. Иметь практический опыт создания педагогических условий для развития группы обучающихся по программам ВО, организационно-методического сопровождения, преподавания для программ бакалавриата, ориентированным на соответствующий уровень квалификации.	Защита ВКР
ПК-5 Способность организовать управление информационной безопасностью	ИПК-5.1. Знать разновидности и свойства систем управления; основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области; технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации; принципы и методы организационной защиты информации, создания систем охранно-тревожной сигнализации, систем контроля и управления доступом, охранного телевидения; принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации; методологию организационной защиты информации, ее современные проблемы и терминологию; основные руководящие документы по обеспечению режима и секретности на объекте; типовую структуру службы безопасности, ее основные задачи и функции должностных лиц; основные документы, регламентирующие организационную безопасность на объекте; правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны; правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации; основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем. ИПК-5.2. Уметь программно реализовывать алгоритмы управления в цифровых системах; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем; пользоваться нормативными документами по защите информации; оценивать состояние организационной защиты информации на объекте; определять рациональные меры по обеспечению организационной защите на объекте; организовать работу с персоналом с секретной (конфиденциальной) информацией; формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости; самостоятельно осуществлять изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности. ИПК-5.3. Владеть навыками работы с нормативными правовыми актами; профессиональной терминологией; навыками формирования методических и нормативных документов, тех. документации в области обеспечения информационной безопасности; знаниями в области правового обеспечения информационной безопасности и навыками правоприменения нормативного законодательства в данной сфере; навыками поиска нормативной и технической информации, необходимой для профессиональной деятельности, обоснования, выбора, реализации и контроля результатов работы; навыками управления информационной безопасностью простых объектов; методами анализа и синтеза систем управления; навыками использования микропроцессоров и микро-ЭВМ в системах управления.	Текст ВКР
ПК-6 Способен обобщать и критически	ИПК-6.1. Знать основные понятия и принципы делопроизводства и электронного документооборота; основные	Текст ВКР

<p>оценивать опыт и результаты научных исследований в области информационной безопасности</p>	<p>стандарты в области инфокоммуникационных систем и технологий; основные отечественные и зарубежные стандарты в области компьютерной безопасности; методологические основы теории принятия решений, теории измерений, теории прогнозирования и планирования; способы измерения свойств объектов предметной области; методы оценки эффективности и качества в задачах прогнозирования, планирования, принятия решений при различной априорной неопределенности имеющейся информации; основные типы статистических задач и математические методы их решения; основные математические методы исследования случайных процессов; основные теоретико-числовые методы применительно к задачам защиты информации; физические основы функционирования технических средств и систем обработки и передачи информации; физические основы образования технических каналов утечки информации; основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; методы концептуального проектирования технологий обеспечения информационной безопасности.</p> <p>ИПК-6.2. Уметь классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; готовить проекты нормативно- распорядительных документов (приказов, указаний, инструкций); готовить проектную документацию на создаваемые специальные АИС; разрабатывать частные политики безопасности компьютерных систем, в том числе, политики управления доступом и информационными потоками; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования; использовать результаты научно-исследовательских работ в решении задач практики; использовать современные модели и методы измерения, прогнозирования, планирования, принятия решений при решении практических задач; самостоятельно строить вероятностные модели применительно к практическим задачам и производить статистическую оценку адекватности полученной модели и реальных задач; применять теоретикочисловые методы для оценки криптографических свойств систем защиты информации; применять системы компьютерной математики для решения типовых задач; использовать физические эффекты для обеспечения технической защиты информации; осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности.</p> <p>ИПК-6.3. Владеть основной юридической терминологией, используемой в гражданском, гражданско- процессуальном, административном, уголовном, уголовно- процессуальном и финансовом законодательстве; навыками письменного аргументированного изложения собственной точки зрения; навыками публичной речи, аргументации, ведения дискуссии и полемики; навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности; основными методами научного познания; навыками использования стандартных методов и моделей математического анализа и их применения к решению прикладных задач; навыками аналитического и численного решения задач математической статистики; методами проведения физического эксперимента при выявлении технических каналов утечки информации.</p>	<p>Защита ВКР</p>
---	--	-------------------

2. Индикаторы оценивания сформированности компетенций

Компетенция	Высокий уровень (отлично) (86-100 баллов)	Средний уровень (хорошо) (71-85 баллов)	Низкий уровень (удовлетворительно) (56-70 баллов)	Ниже порогового уровня (неудовлетворительно) (0-55 баллов)
УК-1	Знает современные и актуальные научные методы для применения системного подхода при построении логических и математических моделей поставленных задач	Знает классические математические методы для применения системного подхода при построении логических и математических моделей поставленных задач	Знает базовые принципы сбора, отбора и обобщения информации в целях проведения построения логических и математических моделей поставленных задач	Не знает базовые принципы сбора, отбора и обобщения информации в целях проведения построения логических и математических моделей поставленных задач
	Умеет проводить системный анализ на основе собранных данных и проектировать новые логические и математические модели для решения поставленных задач	Умеет проводить систематизацию наблюдаемых данных, подбирать адекватные логические и математические модели для решения поставленных задач	Умеет выделять данные, которые необходимо собирать для построения логических и математических моделей поставленных задач, проводить их первичную обработку	Не умеет проводить системный анализ на основе собранных данных и проектировать новые логические и математические модели для решения поставленных задач
	Имеет практический опыт создания научных текстов (статей, тезисов, материалов докладов) на заданную тему	Имеет практический опыт подбора наиболее адекватных источников информации по заданной теме, а также составление обзоров на основе найденных источников	Имеет практический опыт поиска источников информации по заданной теме	Не имеет практический опыт поиска источников информации по заданной теме
УК-2	Знает и умеет корректно применять принципы управления для исследовательских проектов, разрабатываемых на основе различных современных моделях жизненного цикла	Знает принципы управления проектами и особенности из применения для различных этапов жизненного цикла стандартных моделей	Знает принципы управления проектами и особенности из применения для различных этапов жизненного цикла стандартных моделей	Не знает принципы управления проектами и особенности из применения для различных этапов жизненного цикла стандартных моделей
	Умеет рационально планировать собственную профессиональную деятельности с целью получения эффекта от принятия профессиональных решений	Умеет определять и ранжировать задачи выполнения проектов, проводить качественный сравнительный анализ альтернатив	Умеет определять и ранжировать задачи выполнения проектов, проводить качественный сравнительный анализ альтернатив	Не умеет определять и ранжировать задачи выполнения проектов, проводить качественный сравнительный анализ альтернатив
	Владеет навыками разработки и управления исследовательскими проектами в условиях неопределенности, определять оценку эффективности реализации проекта	Владеет навыками ведения и управления исследовательскими проектами, методами оценки потребности в ресурсах, продолжительности, стоимости проекта.	Владеет навыками ведения и управления исследовательскими проектами, методами оценки потребности в ресурсах, продолжительности, стоимости проекта.	Не владеет навыками ведения и управления исследовательскими проектами, методами оценки потребности в ресурсах, продолжительности, стоимости проекта.
УК-3	Знает приемы и способы управления процессом работы в команде	Знает приемы и способы организации работы в команде	Знает базовые приемы и способы социализации личности	Не знает базовые приемы и способы социализации личности
	Умеет строить социальные отношения при управлении профессиональным коллективом	Умеет строить социальные отношения в профессиональном коллективе	Умеет строить социальные отношения с окружающими людьми на основе понимания социальных, личностных особенностей	Не умеет строить социальные отношения с окружающими людьми на основе понимания социальных, личностных особенностей
	Имеет практический опыт управления работы команды при решении задач профессиональной сфере	Имеет практический опыт участия в командной работе при решении задач профессиональной сферы	Имеет практический опыт участия в командной работе в различных социальных проектах	Не имеет практический опыт участия в командной работе в различных социальных проектах

Компетенция	Высокий уровень (отлично) (86-100 баллов)	Средний уровень (хорошо) (71-85 баллов)	Низкий уровень (удовлетворительно) (56-70 баллов)	Ниже порогового уровня (неудовлетворительно) (0-55 баллов)
УК-4	Знает лексический минимум для эффективного осуществления деловой коммуникации в рамках профессиональной деятельности	Знает основные правила современной деловой коммуникации на русском языке и иностранном языке	Знает основные правила современной коммуникации на русском языке и иностранном языке	Не знает основные правила современной коммуникации на русском языке и иностранном языке
	Умеет свободно общаться на русском и иностранном языке для целей профессиональной деятельности	Умеет общаться на русском и иностранном языке для целей профессиональной деятельности, обладает навыками перевода профессионального текста	Умеет общаться на русском и иностранном языке, проводить переводы текстов	Не умеет общаться на русском и иностранном языке, проводить переводы текстов
	Имеет практический опыт составления научных текстов и проектной документации на русском и иностранном языке	Имеет практический опыт составления текстов профессионального характера на русском и иностранном языке	Имеет практический опыт составления текстов на русском и иностранном языке	Не имеет практический опыт составления текстов на русском и иностранном языке
УК-5	Знает и умеет определять место своей профессиональной деятельности с точки зрения социальных, этических и философских контекстов современного общества	Знает философские аспекты и историю развития общества в контексте вопросов организации своей профессиональной деятельности	Знает базовые категории философии, законы исторического развития, основные предпосылки социальных и межкультурных различий	Не знает базовые категории философии, законы исторического развития, основные предпосылки социальных и межкультурных различий
	Умеет обеспечивать и поддерживать взаимопонимание между представителями различных культур и навыки общения в мире культурного многообразия.	Умеет вести коммуникацию с представителями иных национальностей и конфессий с соблюдением этических и межкультурных норм на профессиональные темы	Умеет вести коммуникацию с представителями иных национальностей и конфессий с соблюдением этических и межкультурных норм на повседневные темы	Не умеет вести коммуникацию с представителями иных национальностей и конфессий с соблюдением этических и межкультурных норм на повседневные темы
	Владеет способами анализа разногласий и конфликтов в межкультурной коммуникации и их разрешения.	Имеет практический опыт анализа разногласий и конфликтов в межкультурной коммуникации в ситуациях профессиональной деятельности	Имеет практический опыт анализа разногласий и конфликтов в межкультурной коммуникации в повседневных ситуациях	Не имеет практический опыт анализа разногласий и конфликтов в межкультурной коммуникации в повседневных ситуациях
УК-6	Знает приемы профессионального или личного саморазвития с учетом возможностей карьерного роста и требований рынка труда и собственных целевых установок	Знает основные приемы профессионального и личного саморазвития, ценностные ориентиры на пути достижения более высоких уровней профессионального или личного развития.	Знает основные принципы организации собственного труда, базовые принципы самооценки	Не знает основные принципы организации собственного труда, базовые принципы самооценки
	Умеет анализировать актуальную ситуацию в профессиональной деятельности и определять на ее основе актуальные для себя траектории профессионального развития	Умеет формулировать цели личного и профессионального развития и выявлять условия их достижения	Умеет планировать свое рабочее время и время для саморазвития	Не умеет планировать свое рабочее время и время для саморазвития
	Имеет практический опыт построения и реализации собственной траектории профессионального саморазвития на основе анализа потребностей профессиональной сферы деятельности	Имеет практический опыт самостоятельного изучения новых профессиональных вопросов с помощью дополнительных образовательных программ различных форм	Владеет навыками сбора и ранжирования необходимой для собственного профессионального роста информации, навыками приобретения новых знаний и навыков	Не владеет навыками сбора и ранжирования необходимой для собственного профессионального роста информации, навыками приобретения новых знаний и навыков

Компетенция	Высокий уровень (отлично) (86-100 баллов)	Средний уровень (хорошо) (71-85 баллов)	Низкий уровень (удовлетворительно) (56-70 баллов)	Ниже порогового уровня (неудовлетворительно) (0-55 баллов)
ОПК-1	Отлично знает основные и профессиональные обороты русского и иностранного языков, применяемые при формулировке и доказательстве научных результатов	Сформированные, но содержащие отдельные пробелы представления об основных и профессиональных оборотах русского и иностранного языков, применяемых при формулировке и доказательстве научных результатов	Имеет не полные представления об требованиях нужных для системы обеспечивающую информационную безопасность	Не имеет представления об требованиях нужных для системы обеспечивающую информационную безопасность
	Свободно применяет основные и профессиональные обороты русского и иностранного языка при формулировке и доказательстве научных результатов	Хорошо умеет применять основные и профессиональные обороты русского и иностранного языка при формулировке и доказательстве научных результатов методов	Слабо умеет применять основные и профессиональные обороты русского и иностранного языка при формулировке и доказательстве научных результатов	Не умеет применять основные и профессиональные обороты русского и иностранного языка при формулировке и доказательстве научных результатов
	Свободно владеет основными и профессиональными устными и письменными оборотами русского и иностранного языков при формулировке и доказательстве научных результатов	Достаточно хорошо владеет основными и профессиональными устными и письменными оборотами русского и иностранного языков при формулировке и доказательстве научных результатов	Частично владеет основными и профессиональными устными и письменными оборотами русского и иностранного языков при формулировке и доказательстве научных результатов	Не владеет основными и профессиональными устными и письменными оборотами русского и иностранного языков при формулировке и доказательстве научных результатов
ОПК-2	Знает основные механизмы информационной безопасности и типовые процессы управления этими механизмами в автоматизированной системе; основные угрозы безопасности информации и модели нарушителя в информационных системах; принципы формирования политики информационной безопасности в информационных системах; методы аттестации уровня защищенности информационных систем; основные методы управления информационной безопасностью; физические основы образования технических каналов утечки информации; основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; методы концептуального проектирования технологий обеспечения информационной безопасности.	Знает основные механизмы информационной безопасности и типовые процессы управления этими механизмами в автоматизированной системе; основные угрозы безопасности информации и модели нарушителя в информационных системах; принципы формирования политики информационной безопасности в информационных системах; методы аттестации уровня защищенности информационных систем; основные методы управления информационной безопасностью; физические основы образования технических каналов утечки информации;	Имеет не полные представления об основных механизмах информационной безопасности и типовых процессов управления этими механизмами в автоматизированной системе; имеет не полные представления об основных угрозах безопасности информации и модели нарушителя в информационных системах;	Не знает основные механизмы информационной безопасности и типовые процессы управления этими механизмами в автоматизированной системе; основные угрозы безопасности информации и модели нарушителя в информационных системах;
	Умеет строить системы управления информационной безопасностью в различных условиях функционирования защищаемых автоматизированных систем; раз-	Хорошо умеет строить системы управления информационной безопасностью в различных условиях функционирования защищаемых автоматизированных	Слабо умеет строить системы управления информационной безопасностью в различных условиях функционирования защищаемых автоматизированных сис-	Не умеет строить системы управления информационной безопасностью в различных условиях функционирования защищаемых автоматизированных

Компетенция	Высокий уровень (отлично) (86-100 баллов)	Средний уровень (хорошо) (71-85 баллов)	Низкий уровень (удовлетворительно) (56-70 баллов)	Ниже порогового уровня (неудовлетворительно) (0-55 баллов)
	<p>рабатывать модели угроз и нарушителей информационной безопасности информационных систем; разрабатывать частные политики информационной безопасности информационных систем; контролировать эффективность принятых мер по реализации частных политик информационной безопасности информационных систем; оценивать информационные риски в информационных системах; разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных систем; составлять аналитические обзоры по вопросам обеспечения информационной безопасности информационных систем; применять системы компьютерной математики для решения типовых задач; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности</p>	<p>ных систем; разрабатывать модели угроз и нарушителей информационной безопасности информационных систем; разрабатывать частные политики информационной безопасности информационных систем; контролировать эффективность принятых мер по реализации частных политик информационной безопасности информационных систем; - оценивать информационные риски в информационных системах; разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных систем; составлять аналитические обзоры по вопросам обеспечения информационной безопасности информационных систем;</p>	<p>тем; разрабатывать модели угроз и нарушителей информационной безопасности информационных систем; разрабатывать частные политики информационной безопасности информационных систем; контролировать эффективность принятых мер по реализации частных политик информационной безопасности информационных систем;</p>	<p>систем; разрабатывать модели угроз и нарушителей информационной безопасности информационных систем; разрабатывать частные политики информационной безопасности информационных систем; контролировать эффективность принятых мер по реализации частных политик информационной безопасности информационных систем;</p>
	<p>Владеет методами и средствами выявления угроз безопасности автоматизированным системам; навыками выбора и обоснования критериев эффективности функционирования защищенных информационных систем; навыками участия в экспертизе состояния защищенности информации на объекте защиты; методами управления информационной безопасностью информационных систем; методами оценки информационных рисков; методами организации и управления деятельностью служб защиты информации на предприятии; навыками организации и обеспечения режима секретности навыками управления информационной безопасно-</p>	<p>Достаточно хорошо владеет методами и средствами выявления угроз безопасности автоматизированным системам; навыками выбора и обоснования критериев эффективности функционирования защищенных информационных систем; навыками участия в экспертизе состояния защищенности информации на объекте защиты; методами управления информационной безопасностью информационных систем; методами оценки информационных рисков; методами организации и управления деятельностью служб защиты информации на предприятии; навыками организации и обеспечения</p>	<p>Частично владеет методами и средствами выявления угроз безопасности автоматизированным системам; навыками выбора и обоснования критериев эффективности функционирования защищенных информационных систем; навыками участия в экспертизе состояния защищенности информации на объекте защиты; методами управления информационной безопасностью информационных систем; методами оценки информационных рисков; - методами организации и управления деятельностью служб защиты информации на предприятии; навыками организации и обеспечения режима секретности навыками управления ин-</p>	<p>Не владеет методами и средствами выявления угроз безопасности автоматизированным системам; навыками выбора и обоснования критериев эффективности функционирования защищенных информационных систем; навыками участия в экспертизе состояния защищенности информации на объекте защиты; методами управления информационной безопасностью информационных систем; методами оценки информационных рисков; методами организации и управления деятельностью служб защиты информации на предприятии; навыками организации и обеспечения режима сек-</p>

Компетенция	Высокий уровень (отлично) (86-100 баллов)	Средний уровень (хорошо) (71-85 баллов)	Низкий уровень (удовлетворительно) (56-70 баллов)	Ниже порогового уровня (неудовлетворительно) (0-55 баллов)
	стью простых объектов	режима секретности навыками управления информационной безопасностью простых объектов	формационной безопасностью простых объектов	ретенности навыками управления информационной безопасностью простых объектов
ОПК-3	Знает основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; методы концептуального проектирования технологий обеспечения информационной безопасности; основные нормативные правовые акты в области информационной безопасности и защиты информации; основные понятия, законы, модели и структуры обеспечения организационной безопасности на предприятии; основные понятия, законы и модели прогнозирования принятия решений;	Знает основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; методы концептуального проектирования технологий обеспечения информационной безопасности; основные нормативные правовые акты в области информационной безопасности и защиты информации; понятия, законы, модели и структуры обеспечения организационной безопасности на предприятии	Знает основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; методы концептуального проектирования технологий обеспечения информационной безопасности	Не знает основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; методы концептуального проектирования технологий обеспечения информационной безопасности
	Умеет осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности; использовать нормативные правовые документы в своей профессиональной деятельности; применять основные закономерности принятия управленческих решений и управления коллективом при решении прикладных задач обеспечения информационной безопасности;	Умеет осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности; использовать нормативные правовые документы в своей профессиональной деятельности;	Умеет осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности;	Не умеет осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности;
	Владеет навыками управления информационной безопасностью простых объектов; навыками освоения, внедрения и сопровождения документации, в том числе и в команде; навыками нахождения организационно-управленческих решений в нестандартных ситуациях на основе результатов анализа документации и потоков документов; знаниями в области правового	Владеет навыками управления информационной безопасностью простых объектов; навыками освоения, внедрения и сопровождения документации, в том числе и в команде; навыками нахождения организационно-управленческих решений в нестандартных ситуациях на основе результатов анализа документации и потоков	Владеет навыками управления информационной безопасностью простых объектов; навыками освоения, внедрения и сопровождения документации, в том числе и в команде; навыками нахождения организационно-управленческих решений в нестандартных ситуациях на основе результатов анализа документации и потоков документов; знаниями в	Не владеет навыками управления информационной безопасностью простых объектов; навыками освоения, внедрения и сопровождения документации, в том числе и в команде; навыками нахождения организационно-управленческих решений в нестандартных ситуациях на основе результатов анализа документации и потоков

Компетенция	Высокий уровень (отлично) (86-100 баллов)	Средний уровень (хорошо) (71-85 баллов)	Низкий уровень (удовлетворительно) (56-70 баллов)	Ниже порогового уровня (неудовлетворительно) (0-55 баллов)
	го обеспечения информационной безопасности и навыками правоприменения нормативного законодательства в данной сфере; навыками поиска нормативной и технической информации, необходимой для профессиональной деятельности, обоснования, выбора, реализации и контроля результатов работы	документов; знаниями в области правового обеспечения информационной безопасности и навыками правоприменения нормативного законодательства в данной сфере	области правового обеспечения информационной безопасности и навыками правоприменения нормативного законодательства в данной сфере;	документов; знаниями в области правового обеспечения информационной безопасности и навыками правоприменения нормативного законодательства в данной сфере;
ОПК-4	Знает основные категории и понятия информационно-аналитической работы, принципы и методы ее ведения; источники специальной информации; методы оценивания ее достоверности; виды информационных моделей и способы их построения; методы накопления специальной информации; методы подготовки специальной информации; методы выработки и принятия информационного решения; виды отчетно-информационных документов, методы их подготовки; основные математические методы исследования случайных процессов; основные теоретико-числовые методы применительно к задачам защиты информации; физические основы функционирования технических средств и систем обработки и передачи информации; физические основы образования технических каналов утечки информации; методы концептуального проектирования технологий обеспечения информационной безопасности.	Знает основные категории и понятия информационно-аналитической работы, принципы и методы ее ведения; источники специальной информации; методы оценивания ее достоверности; виды информационных моделей и способы их построения; методы накопления специальной информации; методы подготовки специальной информации; методы выработки и принятия информационного решения; виды отчетно-информационных документов, методы их подготовки;	Знает основные категории и понятия информационно-аналитической работы, принципы и методы ее ведения; источники специальной информации; методы оценивания ее достоверности; виды информационных моделей и способы их построения;	Не знает основные категории и понятия информационно-аналитической работы, принципы и методы ее ведения; источники специальной информации; методы оценивания ее достоверности; виды информационных моделей и способы их построения;
	Умеет использовать руководящие, нормативные и методические документы по организации информационно-аналитической работы; - использовать справочную и научную литературу по тематике решаемых информационных задач; оценивать специальную информацию, систематизировать ее, принимать решения о ее дальнейшем использовании; разрабатывать основные виды отчетно-	Умеет использовать руководящие, нормативные и методические документы по организации информационно-аналитической работы; - использовать справочную и научную литературу по тематике решаемых информационных задач; оценивать специальную информацию, систематизировать ее, принимать решения о ее дальнейшем использовании; разрабатывать основ-	Умеет использовать руководящие, нормативные и методические документы по организации информационно-аналитической работы; - использовать справочную и научную литературу по тематике решаемых информационных задач; оценивать специальную информацию, систематизировать ее, принимать решения о ее дальнейшем использовании; разрабатывать основные виды от-	Не умеет использовать руководящие, нормативные и методические документы по организации информационно-аналитической работы; - использовать справочную и научную литературу по тематике решаемых информационных задач; оценивать специальную информацию, систематизировать ее, принимать решения о ее дальнейшем использовании; разрабатывать основ-

Компетенция	Высокий уровень (отлично) (86-100 баллов)	Средний уровень (хорошо) (71-85 баллов)	Низкий уровень (удовлетворительно) (56-70 баллов)	Ниже порогового уровня (неудовлетворительно) (0-55 баллов)
	информационных документов; применять средства автоматизации информационно-аналитической работы; использовать разнородные источники сведений, отчетно-информационные документы добывающих органов различных видов, в том числе на иностранном языке; применять теоретико-числовые методы для оценки криптографических свойств систем защиты информации; применять системы компьютерной математики для решения типовых задач; использовать физические эффекты для обеспечения технической защиты информации; применять на практике методы физики при исследовании технических каналов утечки информации; осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности.	ные виды отчетно-информационных документов; применять средства автоматизации информационно-аналитической работы; использовать разнородные источники сведений, отчетно-информационные документы добывающих органов различных видов, в том числе на иностранном языке; применять теоретико-числовые методы для оценки криптографических свойств систем защиты информации; применять системы компьютерной математики для решения типовых задач; использовать физические эффекты для обеспечения технической защиты информации; применять на практике методы физики при исследовании технических каналов утечки информации; осуществлять выбор функциональной структуры системы обеспечения информационной безопасности;	четно-информационных документов; применять средства автоматизации информационно-аналитической работы; использовать разнородные источники сведений, отчетно-информационные документы добывающих органов различных видов, в том числе на иностранном языке;	ные виды отчетно-информационных документов; применять средства автоматизации информационно-аналитической работы; использовать разнородные источники сведений, отчетно-информационные документы добывающих органов различных видов, в том числе на иностранном языке;
	Владеет основными системными подходами к определению целей, задач информационно-аналитической работы и источников специальной информации; информацией о современных и перспективных системах автоматизации информационно-аналитической работы; навыками аналитического и численного решения задач математической статистики; методами проведения физического эксперимента при выявлении технических каналов утечки информации.	Владеет основными системными подходами к определению целей, задач информационно-аналитической работы и источников специальной информации; информацией о современных и перспективных системах автоматизации информационно-аналитической работы; навыками аналитического и численного решения задач математической статистики;	Владеет основными системными подходами к определению целей, задач информационно-аналитической работы и источников специальной информации; информацией о современных и перспективных системах автоматизации информационно-аналитической работы;	Не владеет основными системными подходами к определению целей, задач информационно-аналитической работы и источников специальной информации; информацией о современных и перспективных системах автоматизации информационно-аналитической работы;
ОПК-5	Знает основные классификационные признаки экспериментов; основные элементы научно-технического эксперимента; приемы выбора основных факторов экспери-	Знает основные классификационные признаки экспериментов; основные элементы научно-технического эксперимента; приемы выбора основных факто-	Знает основные классификационные признаки экспериментов; основные элементы научно-технического эксперимента; приемы выбора основных факто-	Знает основные классификационные признаки экспериментов; основные элементы научно-технического эксперимента; приемы выбора основных факто-

Компетенция	Высокий уровень (отлично) (86-100 баллов)	Средний уровень (хорошо) (71-85 баллов)	Низкий уровень (удовлетворительно) (56-70 баллов)	Ниже порогового уровня (неудовлетворительно) (0-55 баллов)
	мента и технологию построения факторных планов, основные виды регрессионных экспериментов, основные типы оптимальных экспериментов; основные типы статистических задач и математические методы их решения; основные математические методы исследования случайных процессов; основные теоретико-числовые методы применительно к задачам защиты информации; физические основы функционирования технических средств и систем обработки и передачи информации; физические основы образования технических каналов утечки информации; основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; методы концептуального проектирования технологий обеспечения информационной безопасности.	факторов эксперимента и технологию построения факторных планов, основные виды регрессионных экспериментов, основные типы оптимальных экспериментов; основные типы статистических задач и математические методы их решения; основные математические методы исследования случайных процессов; основные теоретико-числовые методы применительно к задачам защиты информации; физические основы функционирования технических средств и систем обработки и передачи информации;	ров эксперимента и технологию построения факторных планов, основные виды регрессионных экспериментов, основные типы оптимальных экспериментов; основные типы статистических задач и математические методы их решения;	факторов эксперимента и технологию построения факторных планов, основные виды регрессионных экспериментов, основные типы оптимальных экспериментов; основные типы статистических задач и математические методы их решения;
	Умеет проводить классификацию экспериментов; выбирать необходимые факторы и составлять факторные планы экспериментов различного вида; строить системы базисных функций, делать точечные оценки параметров регрессионной модели; анализировать свойства оценок параметров регрессионной модели; выполнять оптимальное планирование экспериментов с использованием различных критериев; самостоятельно строить вероятностные модели применительно к практическим задачам и производить статистическую оценку адекватности полученной модели и реальных задач; применять теоретико-числовые методы для оценки криптографических свойств систем защиты информации; применять системы компьютерной математики для решения типовых задач; использовать физические эффекты для обеспечения технической защиты инфор-	Умеет проводить классификацию экспериментов; выбирать необходимые факторы и составлять факторные планы экспериментов различного вида; строить системы базисных функций, делать точечные оценки параметров регрессионной модели; анализировать свойства оценок параметров регрессионной модели; выполнять оптимальное планирование экспериментов с использованием различных критериев; самостоятельно строить вероятностные модели применительно к практическим задачам и производить статистическую оценку адекватности полученной модели и реальных задач;	Умеет проводить классификацию экспериментов; выбирать необходимые факторы и составлять факторные планы экспериментов различного вида; строить системы базисных функций, делать точечные оценки параметров регрессионной модели; анализировать свойства оценок параметров регрессионной модели; выполнять оптимальное планирование экспериментов с использованием различных критериев;	Не умеет проводить классификацию экспериментов; выбирать необходимые факторы и составлять факторные планы экспериментов различного вида; строить системы базисных функций, делать точечные оценки параметров регрессионной модели; анализировать свойства оценок параметров регрессионной модели; выполнять оптимальное планирование экспериментов с использованием различных критериев;

Компетенция	Высокий уровень (отлично) (86-100 баллов)	Средний уровень (хорошо) (71-85 баллов)	Низкий уровень (удовлетворительно) (56-70 баллов)	Ниже порогового уровня (неудовлетворительно) (0-55 баллов)
	<p>мации; осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности</p>			
	<p>Владеет методами выбора основных факторов эксперимента; методами подбора эмпирических зависимостей для экспериментальных данных; методами оценки коэффициентов регрессионной модели эксперимента; методами построения оптимальных планов для научных экспериментов; навыками аналитического и численного решения задач; методами проведения физического эксперимента при выявлении технических каналов утечки информации</p>	<p>Владеет методами выбора основных факторов эксперимента; методами подбора эмпирических зависимостей для экспериментальных данных; методами оценки коэффициентов регрессионной модели эксперимента; методами построения оптимальных планов для научных экспериментов;</p>	<p>Владеет методами выбора основных факторов эксперимента; методами подбора эмпирических зависимостей для экспериментальных данных; методами оценки коэффициентов регрессионной модели эксперимента;</p>	<p>Не владеет методами выбора основных факторов эксперимента; методами подбора эмпирических зависимостей для экспериментальных данных; методами оценки коэффициентов регрессионной модели эксперимента;</p>
ПК-1	<p>Знает основные теоретико-числовые методы применительно к задачам защиты информации; физические основы функционирования технических средств и систем обработки и передачи информации; физические основы образования технических каналов утечки информации; основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; методы концептуального проектирования технологий обеспечения информационной безопасности</p>	<p>Знает основные теоретико-числовые методы применительно к задачам защиты информации; физические основы функционирования технических средств и систем обработки и передачи информации; физические основы образования технических каналов утечки информации; основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем;</p>	<p>Знает основные теоретико-числовые методы применительно к задачам защиты информации; физические основы функционирования технических средств и систем обработки и передачи информации;</p>	<p>Не знает основные теоретико-числовые методы применительно к задачам защиты информации; физические основы функционирования технических средств и систем обработки и передачи информации;</p>
	<p>Умеет самостоятельно строить вероятностные модели применительно к практическим задачам и производить статистическую оценку адекватности полученной модели и реальных задач; применять теоретико-числовые методы для оценки</p>	<p>Умеет самостоятельно строить вероятностные модели применительно к практическим задачам и производить статистическую оценку адекватности полученной модели и реальных задач; применять теоретико-числовые методы</p>	<p>Умеет самостоятельно строить вероятностные модели применительно к практическим задачам и производить статистическую оценку адекватности полученной модели и реальных задач; применять теоретико-числовые методы для</p>	<p>Не умеет самостоятельно строить вероятностные модели применительно к практическим задачам и производить статистическую оценку адекватности полученной модели и реальных задач; применять теоретико-числовые мето-</p>

Компетенция	Высокий уровень (отлично) (86-100 баллов)	Средний уровень (хорошо) (71-85 баллов)	Низкий уровень (удовлетворительно) (56-70 баллов)	Ниже порогового уровня (неудовлетворительно) (0-55 баллов)
	криптографических свойств систем защиты информации; применять системы компьютерной математики для решения типовых задач; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности	для оценки криптографических свойств систем защиты информации; применять системы компьютерной математики для решения типовых задач; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности	оценки криптографических свойств систем защиты информации	ды для оценки криптографических свойств систем защиты информации
	Владеет навыками аналитического и численного решения задач математической статистики; методами проведения физического эксперимента при выявлении технических каналов утечки информации; навыками управления информационной безопасностью простых объектов.	Владеет навыками аналитического и численного решения задач математической статистики; методами проведения физического эксперимента при выявлении технических каналов утечки информации;	Владеет навыками аналитического и численного решения задач математической статистики;	Не владеет навыками аналитического и численного решения задач математической статистики;
ПК-2	Знает суть методологии и методы научного познания, методы анализа информационных процессов и систем, средства структурного анализа, математические модели информационных процессов; основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; методы концептуального проектирования технологий обеспечения информационной безопасности	Знает суть методологии и методы научного познания, методы анализа информационных процессов и систем, средства структурного анализа, математические модели информационных процессов; основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем	Знает суть методологии и методы научного познания, методы анализа информационных процессов и систем, средства структурного анализа, математические модели информационных процессов	Не знает суть методологии и методы научного познания, методы анализа информационных процессов и систем, средства структурного анализа, математические модели информационных процессов
	Умеет ставить и решать типовые задачи в области структурного анализа информационных процессов и систем, разрабатывать модели предметных областей, проводить исследования характеристик компонентов информационных процессов и информационных систем в целом; осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; организовывать	Умеет ставить и решать типовые задачи в области структурного анализа информационных процессов и систем, разрабатывать модели предметных областей, проводить исследования характеристик компонентов информационных процессов и информационных систем в целом; осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; обосновывать принципы организации технического, программного и информационного обеспечения	Умеет ставить и решать типовые задачи в области структурного анализа информационных процессов и систем, разрабатывать модели предметных областей, проводить исследования характеристик компонентов информационных процессов и информационных систем в целом	Не умеет ставить и решать типовые задачи в области структурного анализа информационных процессов и систем, разрабатывать модели предметных областей, проводить исследования характеристик компонентов информационных процессов и информационных систем в целом

Компетенция	Высокий уровень (отлично) (86-100 баллов)	Средний уровень (хорошо) (71-85 баллов)	Низкий уровень (удовлетворительно) (56-70 баллов)	Ниже порогового уровня (неудовлетворительно) (0-55 баллов)
	работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности	печения информационной безопасности		
	Владеет методами анализа информационных процессов и систем, методами разработки математических моделей информационных процессов; навыками управления информационной безопасностью простых объектов	Владеет методами анализа информационных процессов и систем, методами разработки математических моделей информационных процессов; навыками управления информационной безопасностью простых объектов	Владеет методами анализа информационных процессов и систем, методами разработки математических моделей информационных процессов;	Не владеет методами анализа информационных процессов и систем, методами разработки математических моделей информационных процессов;
ПК-3	Знает основные принципы обеспечения информационной безопасности и защиты информации; структуру систем документационного обеспечения; основные понятия и методы в области управления службой безопасности предприятия; организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации; основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России; понятия и виды защищаемой информации; виды основных угроз защищаемой информации; базовые понятия о методах и средствах защиты информации; международные стандарты информационной безопасности	Знает основные принципы обеспечения информационной безопасности и защиты информации; структуру систем документационного обеспечения; - основные понятия и методы в области управления службой безопасности предприятия; организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации; основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России	Знает основные принципы обеспечения информационной безопасности и защиты информации; структуру систем документационного обеспечения; основные понятия и методы в области управления службой безопасности предприятия; организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации	Не знает основные принципы обеспечения информационной безопасности и защиты информации; структуру систем документационного обеспечения; - основные понятия и методы в области управления службой безопасности предприятия; организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации
	Умеет анализировать и оценивать угрозы информационной безопасности объекта; пользоваться нормативными документами по защите информации; определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы,	Умеет анализировать и оценивать угрозы информационной безопасности объекта; пользоваться нормативными документами по защите информации; - определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; определять комплекс мер (правила, процедуры, практические приемы,	Умеет анализировать и оценивать угрозы информационной безопасности объекта; пользоваться нормативными документами по защите информации; определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите;	Не умеет анализировать и оценивать угрозы информационной безопасности объекта; пользоваться нормативными документами по защите информации; - определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите;

Компетенция	Высокий уровень (отлично) (86-100 баллов)	Средний уровень (хорошо) (71-85 баллов)	Низкий уровень (удовлетворительно) (56-70 баллов)	Ниже порогового уровня (неудовлетворительно) (0-55 баллов)
	<p>средства) для обеспечения информационной безопасности сведений, составляющих государственную и коммерческую тайну; уметь проводить процедуры аттестации, категорирования объектов информатизации; уметь пользоваться научно-технической и справочной литературой для решения прикладных задач; осуществлять поиск информации в Интернет и выполнять аналитического исследования по определенной теме.</p> <p>Владеет навыками анализа методов и средств передачи, хранения и обработки данных, навыками применения средств охраны от негативных воздействий, навыками оценки защищенности объектов информатизации, навыками организации охраны на объектах информатизации, навыками применения технических средств защиты информации; типовыми приемами проектирования, инструментарием для документирования проектных решений, методами прямого и обратного проектирования; навыками анализа информационной инфраструктуры информационной системы и ее безопасности; пользоваться нормативными документами по противодействию технической разведке; применять действующую законодательную базу в области обеспечения информационной безопасности; применять нормативные правовые акты и нормативные методические документы в области обеспечения безопасности сведений, составляющих государственную и коммерческую тайну; владеть методами и средствами защиты информации, применяемыми в деятельности службы безопасности на предприятиях для обеспечения защиты сведений, составляющих государственную и коммерческую тайну</p>	<p>руководящие принципы, методы, средства) для обеспечения информационной безопасности сведений, составляющих государственную и коммерческую тайну;</p> <p>Владеет навыками анализа методов и средств передачи, хранения и обработки данных, навыками применения средств охраны от негативных воздействий, навыками оценки защищенности объектов информатизации, навыками организации охраны на объектах информатизации, навыками применения технических средств защиты информации; типовыми приемами проектирования, инструментарием для документирования проектных решений, методами прямого и обратного проектирования; навыками анализа информационной инфраструктуры информационной системы и ее безопасности; пользоваться нормативными документами по противодействию технической разведке; применять действующую законодательную базу в области обеспечения информационной безопасности;</p>	<p>Владеет навыками анализа методов и средств передачи, хранения и обработки данных, навыками применения средств охраны от негативных воздействий, навыками оценки защищенности объектов информатизации, навыками организации охраны на объектах информатизации, навыками применения технических средств защиты информации; - типовыми приемами проектирования, инструментарием для документирования проектных решений, методами прямого и обратного проектирования;</p>	<p>Не владеет навыками анализа методов и средств передачи, хранения и обработки данных, навыками применения средств охраны от негативных воздействий, навыками оценки защищенности объектов информатизации, навыками организации охраны на объектах информатизации, навыками применения технических средств защиты информации; типовыми приемами проектирования, инструментарием для документирования проектных решений, методами прямого и обратного проектирования;</p>

Компетенция	Высокий уровень (отлично) (86-100 баллов)	Средний уровень (хорошо) (71-85 баллов)	Низкий уровень (удовлетворительно) (56-70 баллов)	Ниже порогового уровня (неудовлетворительно) (0-55 баллов)
ПК-4	Знает, анализирует, выявляет наилучшие современные педагогические условия для развития группы обучающихся по программам ВО, организационно-методическое сопровождение, преподавание для программ бакалавриата, ориентированным на соответствующий уровень квалификации	Знает современные педагогические условия для развития группы обучающихся по программам ВО, организационно-методическое сопровождение, преподавание для программ бакалавриата, ориентированным на соответствующий уровень квалификации	Знает базовые педагогические условия для развития группы обучающихся по программам ВО, организационно-методическое сопровождение, преподавание для программ бакалавриата, ориентированным на соответствующий уровень квалификации	Не знает базовые педагогические условия для развития группы обучающихся по программам ВО, организационно-методическое сопровождение, преподавание для программ бакалавриата, ориентированным на соответствующий уровень квалификации
	Умеет под руководством специалиста более высокой квалификации разрабатывать и проводить практические занятия (семинары) со студентами-бакалаврами; самостоятельно осуществлять организационно-методическое сопровождение; анализировать проведенное занятие	Умеет под руководством специалиста более высокой квалификации разрабатывать и проводить практические занятия (семинары) со студентами-бакалаврами; осуществлять организационно-методическое сопровождение	Умеет под руководством специалиста более высокой квалификации разрабатывать и проводить практические занятия (семинары) со студентами-бакалаврами	Не умеет под руководством специалиста более высокой квалификации разрабатывать и проводить практические занятия (семинары) со студентами-бакалаврами
	Имеет практический опыт под руководством специалиста более высокой квалификации разработки и проведения практических занятий (семинары) со студентами-бакалаврами с последующим анализом и обсуждением; осуществления организационно-методического сопровождения	Имеет практический опыт под руководством специалиста более высокой квалификации разработки и проведения практических занятий (семинары) со студентами-бакалаврами; осуществления организационно-методического сопровождения	Имеет практический опыт под руководством специалиста более высокой квалификации разработки и проведения практических занятий (семинары) со студентами-бакалаврами	Не имеет практический опыт под руководством специалиста более высокой квалификации разработки и проведения практических занятий (семинары) со студентами-бакалаврами
ПК-5	Знает разновидности и свойства систем управления; основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области; технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации; принципы и методы организационной защиты информации, создания систем охранно-тревожной сигнализации, систем контроля и управления доступом, охранного телевидения; принципы и методы противодействия несанкционированному информационному воздействию на вычис-	Знает разновидности и свойства систем управления; основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области; технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации; - принципы и методы организационной защиты информации, создания систем охранно-тревожной сигнализации, систем контроля и управления доступом, охранного телевидения; принципы и методы противо-	Знает разновидности и свойства систем управления; основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области; технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации	Не знает разновидности и свойства систем управления; - основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области; технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации

Компетенция	Высокий уровень (отлично) (86-100 баллов)	Средний уровень (хорошо) (71-85 баллов)	Низкий уровень (удовлетворительно) (56-70 баллов)	Ниже порогового уровня (неудовлетворительно) (0-55 баллов)
	<p>лительные системы и системы передачи информации; методологию организационной защиты информации, ее современные проблемы и терминологию; основные руководящие документы по обеспечению режима и секретности на объекте; типовую структуру службы безопасности, ее основные задачи и функции должностных лиц; основные документы, регламентирующую организационную безопасность на объекте; правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны; правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации; основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем</p>	<p>действия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации; методологию организационной защиты информации, ее современные проблемы и терминологию</p>		
	<p>Умеет программно реализовывать алгоритмы управления в цифровых системах; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем; пользоваться нормативными документами по защите информации; оценивать состояние организационной защиты информации на объекте; определять рациональные меры по обеспечению организационной защите на объекте; организовать работу с персоналом с секретной (конфиденциальной) информацией; формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости; самостоятельно осуществлять изучение и обобщение научно-технической</p>	<p>Умеет программно реализовывать алгоритмы управления в цифровых системах; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем; пользоваться нормативными документами по защите информации; оценивать состояние организационной защиты информации на объекте; определять рациональные меры по обеспечению организационной защите на объекте; организовать работу с персоналом с секретной (конфиденциальной) информацией; формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости</p>	<p>Умеет программно реализовывать алгоритмы управления в цифровых системах; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем; пользоваться нормативными документами по защите информации; оценивать состояние организационной защиты информации на объекте; определять рациональные меры по обеспечению организационной защите на объекте;</p>	<p>Не умеет программно реализовывать алгоритмы управления в цифровых системах; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем; пользоваться нормативными документами по защите информации; оценивать состояние организационной защиты информации на объекте; определять рациональные меры по обеспечению организационной защите на объекте</p>

Компетенция	Высокий уровень (отлично) (86-100 баллов)	Средний уровень (хорошо) (71-85 баллов)	Низкий уровень (удовлетворительно) (56-70 баллов)	Ниже порогового уровня (неудовлетворительно) (0-55 баллов)
	<p>литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности</p> <p>Владеет навыками работы с нормативными правовыми актами; профессиональной терминологией; навыками формирования методических и нормативных документов, тех. документации в области обеспечения информационной безопасности; знаниями в области правового обеспечения информационной безопасности и навыками правоприменения нормативного законодательства в данной сфере; навыками поиска нормативной и технической информации, необходимой для профессиональной деятельности, обоснования, выбора, реализации и контроля результатов работы; навыками управления информационной безопасностью простых объектов; методами анализа и синтеза систем управления; навыками использования микропроцессоров и микро-ЭВМ в системах управления</p>	<p>Владеет навыками работы с нормативными правовыми актами; профессиональной терминологией; навыками формирования методических и нормативных документов, тех. документации в области обеспечения информационной безопасности; знаниями в области правового обеспечения информационной безопасности и навыками правоприменения нормативного законодательства в данной сфере; навыками поиска нормативной и технической информации, необходимой для профессиональной деятельности, обоснования, выбора, реализации и контроля результатов работы;</p>	<p>Владеет навыками работы с нормативными правовыми актами; профессиональной терминологией; навыками формирования методических и нормативных документов, тех. документации в области обеспечения информационной безопасности; знаниями в области правового обеспечения информационной безопасности и навыками правоприменения нормативного законодательства в данной сфере;</p>	<p>Не владеет навыками работы с нормативными правовыми актами; профессиональной терминологией; навыками формирования методических и нормативных документов, тех. документации в области обеспечения информационной безопасности; знаниями в области правового обеспечения информационной безопасности и навыками правоприменения нормативного законодательства в данной сфере;</p>
ПК-6	<p>Знает основные понятия и принципы делопроизводства и электронного документооборота; основные стандарты в области инфокоммуникационных систем и технологий; основные отечественные и зарубежные стандарты в области компьютерной безопасности; методологические основы теории принятия решений, теории измерений, теории прогнозирования и планирования; способы измерения свойств объектов предметной области; методы оценки эффективности и качества в задачах прогнозирования, планирования, принятия решений при различной априорной неопределенности имеющейся информа-</p>	<p>Знает основные понятия и принципы делопроизводства и электронного документооборота; основные стандарты в области инфокоммуникационных систем и технологий; основные отечественные и зарубежные стандарты в области компьютерной безопасности; методологические основы теории принятия решений, теории измерений, теории прогнозирования и планирования; способы измерения свойств объектов предметной области; методы оценки эффективности и качества в задачах прогнозирования, планирования, принятия решений при различной</p>	<p>Знает основные понятия и принципы делопроизводства и электронного документооборота; основные стандарты в области инфокоммуникационных систем и технологий; основные отечественные и зарубежные стандарты в области компьютерной безопасности; методологические основы теории принятия решений, теории измерений, теории прогнозирования и планирования; способы измерения свойств объектов предметной области; методы оценки эффективности и качества в задачах прогнозирования, планирования, принятия решений при различной априорной неопределенности</p>	<p>Не знает основные понятия и принципы делопроизводства и электронного документооборота; основные стандарты в области инфокоммуникационных систем и технологий; основные отечественные и зарубежные стандарты в области компьютерной безопасности; методологические основы теории принятия решений, теории измерений, теории прогнозирования и планирования; способы измерения свойств объектов предметной области; методы оценки эффективности и качества в задачах прогнозирования, планирования, принятия решений при различной</p>

Компетенция	Высокий уровень (отлично) (86-100 баллов)	Средний уровень (хорошо) (71-85 баллов)	Низкий уровень (удовлетворительно) (56-70 баллов)	Ниже порогового уровня (неудовлетворительно) (0-55 баллов)
	ции; основные типы статистических задач и математические методы их решения; основные математические методы исследования случайных процессов; основные теоретико-числовые методы применительно к задачам защиты информации; физические основы функционирования технических средств и систем обработки и передачи информации; физические основы образования технических каналов утечки информации; основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; методы концептуального проектирования технологий обеспечения информационной безопасности	априорной неопределенности имеющейся информации; основные типы статистических задач и математические методы их решения; основные математические методы исследования случайных процессов; основные теоретико-числовые методы применительно к задачам защиты информации; физические основы функционирования технических средств и систем обработки и передачи информации	имеющейся информации	априорной неопределенности имеющейся информации
	Умеет классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; готовить проекты нормативно-распорядительных документов (приказов, указаний, инструкций); готовить проектную документацию на создаваемые специальные АИС; разрабатывать частные политики безопасности компьютерных систем, в том числе, политики управления доступом и информационными потоками; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования; использовать результаты научно-исследовательских работ в решении задач практики; использовать современные модели и методы измерения, прогнозирования, планирования, принятия решений при решении практических задач; самостоятельно строить вероятностные модели применительно к практическим задачам и производить статистическую оценку адекватности полученной модели и реальных задач; применять теоретико-числовые	Умеет классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; готовить проекты нормативно-распорядительных документов (приказов, указаний, инструкций); готовить проектную документацию на создаваемые специальные АИС; разрабатывать частные политики безопасности компьютерных систем, в том числе, политики управления доступом и информационными потоками; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования; использовать результаты научно-исследовательских работ в решении задач практики; использовать современные модели и методы измерения, прогнозирования, планирования, принятия решений при решении практических задач; самостоятельно строить вероятностные модели применительно к практическим задачам и производить статистическую оценку	Умеет классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; готовить проекты нормативно-распорядительных документов (приказов, указаний, инструкций); готовить проектную документацию на создаваемые специальные АИС; разрабатывать частные политики безопасности компьютерных систем, в том числе, политики управления доступом и информационными потоками; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования	Не умеет классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; готовить проекты нормативно-распорядительных документов (приказов, указаний, инструкций); готовить проектную документацию на создаваемые специальные АИС; разрабатывать частные политики безопасности компьютерных систем, в том числе, политики управления доступом и информационными потоками; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования

Компетенция	Высокий уровень (отлично) (86-100 баллов)	Средний уровень (хорошо) (71-85 баллов)	Низкий уровень (удовлетворительно) (56-70 баллов)	Ниже порогового уровня (неудовлетворительно) (0-55 баллов)
	<p>методы для оценки криптографических свойств систем защиты информации; применять системы компьютерной математики для решения типовых задач; использовать физические эффекты для обеспечения технической защиты информации; осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности</p>	<p>адекватности полученной модели и реальных задач</p>		
	<p>Владеет методами решения задач с помощью аппарата математического анализа, методами линейной алгебры, методы решения, теорией линейных операторов, численными методами, навыками практического использования математического аппарата дисциплины для решения конкретных задач</p>	<p>Владеет методами решения задач с помощью аппарата математического анализа, методами линейной алгебры, методы решения, теорией линейных операторов, численными методами</p>	<p>Владеет методами решения задач с помощью аппарата математического анализа, методами линейной алгебры, методы решения, теорией линейных операторов</p>	<p>Не владеет методами решения задач с помощью аппарата математического анализа, методами линейной алгебры, методы решения, теорией линейных операторов</p>

3. Механизм формирования оценки за выпускную квалификационную работу

3.1. Механизм формирования оценки для обучающихся очной и очно-заочной форм обучения (с применением балльно-рейтинговой системы).

Оценка за ВКР формируется суммой баллов за текст ВКР и за защиту ВКР.

Баллы в интервале 86-100 – отлично (высокий уровень)

Баллы в интервале 71-85 – хорошо (средний уровень)

Баллы в интервале 56-70 – удовлетворительно (низкий уровень)

Баллы в интервале 0-55 – неудовлетворительно (ниже порогового уровня)

Если балл за сформированность хотя бы одной компетенции находится ниже порогового уровня, ВКР считается незащищенной.

ВКР считается защищенной при получении баллов, соответствующих оценке не менее «удовлетворительно», как за текст ВКР, так и за защиту ВКР.

За текст ВКР обучающийся может заработать 80 баллов максимум, за защиту ВКР – 20 баллов максимум.

Каждый параметр в пункте 4.3., относящийся к тексту ВКР, оценивается максимально в 80 баллов. Средний балл за оценку всех параметров является баллом за текст ВКР.

Каждый параметр в пункте 4.3., относящийся к защите ВКР, оценивается максимально в 20 баллов. Средний балл за оценку всех параметров является баллом за защиту ВКР.

Параметры в пункте 4.3, относящиеся к оценке результатов промежуточной аттестации и (или) портфолио обучающегося (при наличии), оцениваются каждый максимально в 20 баллов и являются составными элементами при формировании среднего балла за защиту ВКР.

В отзыве и рецензии дается качественная рекомендация, по оценке выпускной квалификационной работы. Рекомендация учитывается комиссией при выставлении баллов за текст ВКР – может быть произведено снижение баллов за замечания и более низкую оценку руководителя и/или рецензента.

По каждому обучающемуся составляется Оценочный лист по подготовке к сдаче и сдаче выпускной квалификационной работы, оформляемый по форме Приложения 2 к программе подготовки к защите и защиты выпускной квалификационной работы. Оценочный лист является приложением к соответствующему Протоколу заседания ГЭК и хранится вместе с текстом ВКР.

4. Оценочные средства, порядок их применения и критерии оценивания

4.1. Процедура применения оценочного средства

4.1.1. Процедура оценивания текста выпускной квалификационной работы

Руководитель ВКР оценивает:

1) процесс работы обучающегося над ВКР в течение учебного года, включая своевременность выполнения этапов работы, уровень проведенных исследований, частоту консультаций, своевременность написания текста ВКР и др.;

2) текст ВКР, включая его структуру, содержание и оформление.

Оценивание руководителем работы обучающегося над ВКР в течение учебного года производится на основании личного взаимодействия с обучающимся, в том числе дистанционного, и ознакомления с промежуточными результатами работы. Оценивание текста ВКР производится на основании ознакомления с окончательным вариантом текста ВКР.

Руководитель отражает в отзыве свою оценку по каждому из параметров оценивания текста ВКР, указанных в пункте 4.3 настоящего фонда оценочных средств.

Рецензент оценивает текст ВКР, включая его структуру, содержание и оформление, на основании ознакомления с беловым вариантом текста ВКР. Рецензент отражает в рецензии свою оценку по каждому из параметров оценивания текста ВКР, указанных в пункте 4.3 настоящего фонда оценочных средств, за исключением тех, которые относятся к процессу работы над ВКР и не могут быть оценены на основании знакомства исключительно с ее текстом.

Председатель и члены государственной экзаменационной комиссии оценивают текст ВКР, включая его структуру, содержание и оформление, при непосредственном знакомстве с ним во время защиты ВКР. Они учитывают оценки, данные руководителем ВКР и рецензентом, в соответствии с механизмом формирования оценки за ВКР, указанным в пункте 3 настоящего фонда оценочных средств.

4.1.2. Процедура оценивания защиты выпускной квалификационной работы

Защита выпускной квалификационной работы включает в себя выступление обучающегося, а также ответы на вопросы рецензента и членов ГЭК. На выступление обучающемуся дается 10 минут. После выступления обучающийся отвечает на вопросы комиссии. Далее оглашаются письменные отзывы руководителя и рецензента, после чего автор работы отвечает на имеющиеся в отзывах вопросы и замечания.

Решение государственной экзаменационной комиссии принимается на закрытом заседании. При расхождении мнений членов комиссии оценка определяется путём голосования простым большинством голосов, при равном количестве голосов голос председателя комиссии (при его отсутствии – заместителя председателя) является решающим. Оценка по ВКР объявляется после защиты и выставляется в протоколе заседания государственной экзаменационной комиссии и в зачетной книжке обучающегося.

4.2. Требования к выпускной квалификационной работе

4.2.1. Требования к тексту выпускной квалификационной работы

Работа обучающегося в течение учебного года состоит из следующих этапов:

1. выбор темы выпускной квалификационной работы;
2. работа с научным руководителем по определению цели и основных задач исследования, дальнейшие консультации;
3. поиск и сбор информации для исследований и разработок;
4. основной этап выполнения выпускной квалификационной работы, включающий в зависимости от темы работы инфокоммуникации в специальной робототехнике, современные алгоритмы и средства решения задач обеспечения информационной безопасности с помощью теоретического анализа или проведения экспериментов с помощью специально разработанного программного обеспечения;
5. оформление текста выпускной квалификационной работы;
6. подготовка к защите выпускной квалификационной работы.

Обучающийся своевременно, сразу после распределения тем (осенью), начинает посещать консультации научного руководителя, совместно с научным руководителем формулирует (уточняет) тему и задачи исследования. В течение всего учебного года периодически представляет научному руководителю промежуточные результаты работы. Обучающийся учитывает пожелания и замечания научного руководителя, корректируя текст. Корректировка темы согласуется с научным руководителем. Финальный вариант работы предоставляет научному руководителю в такие сроки, чтобы оставшегося времени хватило для внесения корректив в соответствии с замечаниями научного руководителя.

Структурными элементами ВКР являются:

- титульный лист;
- содержание;
- введение;
- основная часть, состоящая из глав, которые делятся на параграфы, или из разделов без дальнейшего деления на части;
- заключение;
- список использованных источников;
- приложения (при необходимости).

Объем ВКР – не менее 30 страниц машинописного текста (не считая приложений). Соотношение частей работы должно быть сбалансировано по объему. Объем приложений не ограничивается. Формат: страница А4; поля не более чем: 3 см слева, по 2 см сверху и снизу, 1,5 см справа; шрифт TimesNewRoman; размер шрифта не более 14; не более чем полуторный интервал. Объем работы не раздут искусственно (слишком большие поля, шрифт и интервал, каждый параграф с новой страницы при большом количестве параграфов).

Во введении:

- обосновывается актуальность выбранной темы;
- производится обзор литературы по теме (он может быть также перенесен в основную часть);
- формулируется проблема, которую необходимо решить в данной работе;
- определяются цель и задачи исследования.

Рекомендуемый объем введения – 3-5 страниц.

Основная часть разделена на главы и разделы. Деление должно обуславливаться тематикой выпускной квалификационной работы. Рекомендуется использовать деление на три главы - теоретическое описание предлагаемых методик (для работ исследовательской направленности) или описание предметной области прикладной разработки, описание программной реализации и экспериментальная глава.

В заключении последовательно излагаются теоретические и практические результаты и суждения, к которым пришел обучающийся в результате исследования. Они должны быть краткими, четкими, дающими полное представление о содержании, значимости, обоснованности и эффективности работы. Результаты (выводы) исследования должны соответствовать поставленным цели и задачам.

Список использованной литературы составляет одну из важных частей работы. Каждый включенный литературный источник должен иметь отражение в тексте выпускной квалификационной работы. Если автор делает ссылку на какие-либо заимствованные факты или цитирует работы других авторов, то он должен указать, откуда взяты приведенные материалы. Нельзя включать в библиографический список те работы, на которые нет ссылок в тексте работы, и которые фактически не были использованы.

В библиографии присутствуют в достаточном количестве работы, опубликованные в научных издательствах (научные монографии, статьи в научных журналах, материалы научных конференций). Недостаточно ссылаться только на материалы Интернета, авторитетность и научность которых не определена. Недопустимо ссылаться на материалы Интернета, размещенные там без указания авторства.

Использованная литература соответствует теме. Источники, относящиеся не непосредственно к теме, а к смежным, близким темам, не составляют основного массива использованной литературы.

В число использованных источников входят публикации достойного научного уровня, которые можно отнести к числу наиболее значительных для тематической области работы.

Все публикации, указанные в библиографии, используются в тексте – путем цитирования и/или пересказа идей своими словами, но обязательно с проставлением сносок.

Приложения призваны облегчить восприятие содержания работы и могут включать: дополнительные материалы, иллюстрации вспомогательного характера, программный код разработанного приложения и др.

Структура работы логически выверена. Название параграфа не дублирует название главы или работы в целом, то же с названиями глав. Разделы (главы, параграфы) сопоставимы по объему. Части работы в своей совокупности раскрывают тему работы. Все части работы вписываются в тему, работают на достижение цели исследования, заявленной во введении. Содержание работы не шире и не уже, чем заявленная тема; то же касается каждого раздела (главы, параграфа). Последовательность рассмотрения вопросов логически оправдана. Прочерчены взаимосвязи между частями работы, вместе они образуют единую систему.

Текст ВКР должен быть написан грамотным русским языком, с соблюдением норм академического стиля. Изложение идей должно быть логичным, последовательным, связным, сопровождаться аргументацией.

На титульном листе указываются: наименование Министерства науки и высшего образования Российской Федерации, полное наименование организации (КФУ), института / факультета, отделения (при наличии), название темы, информация об обучающемся – авторе ВКР (ФИО, номер группы, шифр и наименование направления подготовки (специальности) и профиля, информация о руководителе ВКР (ФИО, ученая степень, ученое звание, должность), город и год защиты.

Процент самостоятельности текста ВКР, определенный автоматическими программными средствами обнаружения заимствований, должен составлять не менее 60 %.

4.2.2. Требования к защите выпускной квалификационной работы

Предварительная подготовка обучающегося к защите ВКР в себя ряд этапов:

- Составление текста выступления перед государственной экзаменационной комиссией. Выступление, рассчитанное на 10 минут, составляется на основе введения, выводов по главам и заключения. В тексте выступления необходимо показать результативность выполненного исследования. Вся информация, которая прозвучит в выступлении, должна быть идентичной той, которая содержится в ВКР: содержать ту же терминологию, раскрывать те же задачи.

- Изготовление иллюстративных материалов, используемых в процессе защиты. Это могут быть схемы, графики, дающие наглядное представление о специфике проведенного исследования. Компьютерный вариант презентации материалов выполняется средствами программы MS PowerPoint.

- Продумывание ответов на замечания, содержащихся в отзыве рецензента.

- Подготовка для членов комиссии листов-презентаций (в соответствии с количеством членов комиссии), содержащих основные методологические характеристики работы: тема, цель, объект и предмет исследования, задачи и методы исследования, база исследования, его практическая значимость.

Защита ВКР проводится на открытом заседании государственной экзаменационной комиссии с участием не менее двух третей ее состава. Защита является публичной, т.к. заседание открытое и в нем могут принимать участие все желающие преподаватели и обучающиеся. На защите руководитель ВКР и рецензент пользуются правом совещательного голоса.

Процесс защиты ВКР включает:

- Выступление обучающегося.

- Ответы на вопросы. По окончании выступления обучающийся отвечает на вопросы. Вопросы по содержанию работы могут быть заданы не только членами комиссии, но и всеми присутствующими на защите. Желательно отвечать спокойно, без лишней эмоциональности, немногословно, вместе с тем дать исчерпывающий ответ.

- Зачитывается заключение рецензента.

- Обучающемуся предоставляется право ответить на вопросы и замечания, содержащиеся в рецензии. Обучающийся должен ответить на все критические замечания рецензента и обосновать свою позицию по тем вопросам, в трактовке которых он с замечанием рецензента не согласен.

- Зачитывается отзыв научного руководителя.

- Обучающемуся предоставляется заключительное слово. Здесь обучающийся может сказать о том, чем привлекла его именно эта тема, что было особенно интересным в процессе выполнения дипломного исследования и т.д.

В целом на всю процедуру защиты отводится не более 30 минут.

Комиссия удаляется на совещание, после которой объявляются отметки, выставленные за ВКР. Оценка за ВКР вместе с темой работы вносится в Приложение к диплому.

Ход заседания комиссии протоколируется. В протоколе фиксируется: итоговая оценка ВКР, вопросы и особые мнения членов комиссии. Протоколы заседаний комиссии подписываются председателем, заместителем председателя, ответственным секретарем и членами комиссии.

Рекомендации к электронной презентации выпускной квалификационной работе:

- Электронная презентация сопровождает доклад обучающегося о ходе и результатах научного исследования в ходе публичной защиты ВКР.

- Содержание презентации может совпадать с текстом выступления, но не дублировать его. Основной целью презентации является комплексное представление проблемного поля исследования и его результатов.

Объем презентации определяется общей длительностью выступления (8-10 минут) и составляет не менее 15 слайдов.

Часть слайдов может быть ориентирована только на визуальное восприятие и сопровождаться минимальными устными комментариями в ходе выступления (например, в устном комментарии слайда «Проблема исследования, цель исследования, объект исследования, предмет исследования» выступающий называет только цель исследования, проблема, объект и предмет исследования воспринимается только визуально; гипотеза исследования озвучивается, а в комментарии слайда «Задачи исследования» говорится, что задачи исследования представлены на слайде (каждая задача называется позже в логике устного выступления, рекомендуется строить устное выступление по задачам ВКР).

Презентация должна быть подготовлена в программной среде Microsoft PowerPoint.

Фон слайдов должен быть единым для всей презентации, иметь деловой, психологически комфортный стиль, соответствующий формату мероприятия. Не рекомендуется использовать типовые шаблоны фона с графическими изображениями или рисунками. Если в качестве фона отдельных слайдов используется изображение, то степень его яркости не должна мешать четкому восприятию графических объектов и чтению текста.

Текст, размещаемый на слайде, должен быть лаконичен и ограничен по общему объему. Рекомендуется оформлять текст в виде тезисов и маркированных (пронумерованных) положений, а также широко использовать графические объекты (схемы, таблицы, графики, диаграммы). Слайды не должны иметь подзаголовков, дублирующих содержание информационных объектов.

Текст оформляется шрифтом не менее 20 pt (в отдельных случаях (если на слайд не помещается небольшое количество оставшегося текста) шрифт может быть уменьшен до 18). Возможно выделение текста полужирным шрифтом, но не рекомендуется использование курсива. Форматирование текста осуществляется по ширине. Рекомендуемый шрифт – TimesNewRoman. Оптимальной цветовой комбинацией шрифта и фона являются «темные буквы на белом фоне». В тексте может быть сделано логическое ударение – выделение слова или словосочетания цветом.

В тексте должны быть соблюдены принятые правила орфографии, пунктуации, сокращения и специальные правила оформления (например, отсутствие точки в заголовках).

Схемы, таблицы, графики и диаграммы, включенные в состав презентации, либо выполняют самостоятельные информативные функции, либо иллюстрируют конкретные тезисы выступления, посвященные содержанию и выводам ВКР. Цветовое оформление графических объектов должно быть соразмерным общей цветовой гамме (рекомендуется использовать не более трех цветов в рамках всей презентации).

Используемые в составе презентации иллюстративные изображения (репродукции картин, плакаты, фотографии, рисунки и т.п.) должны быть связаны с конкретными содержательными элементами презентации. Все изображения должны иметь максимально большое разрешение (не допускается «растянутое» изображение слабого разрешения). При размещении на слайдах изображение необходимо «растягивать» только через «угол», чтобы не нарушить его пропорции. Каждое изображение должно иметь подпись, корректно и грамотно отражающую его выходные данные.

Анимационные эффекты могут быть применены к графическим объектам (схемам, таблицам, графикам и диаграммам) и изображениям, если это необходимо для поэтапного восприятия материала. Для оформления базовой информации использование анимационных эффектов не рекомендуется.

В качестве отдельных элементов презентации могут быть использованы аудио- и видеоматериалы. Длительность каждого из таких фрагментов должна быть строго ограничена. Интенсивность звука должна быть комфортной для аудитории. Не допускается использование музыки в качестве постоянного фона.

4.3. Критерии оценивания выпускной квалификационной работы

Шифр и расшифровка компетенции	Индикаторы достижений компетенций, раскрываемые параметром	Параметр	Критерии оценивания			
			Баллы в интервале 86-100 % (высокий уровень, отлично) от максимальных ставятся в случае, если:	Баллы в интервале 71-85% (средний уровень, хорошо) от максимальных ставятся в случае, если:	Баллы в интервале 56-70% (низкий уровень, удовлетворительно) от максимальных ставятся в случае, если:	Баллы в интервале 0-55% (ниже порогового уровня, неудовлетворительно) от максимальных ставятся в случае, если:
Текст ВКР						
УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	ИУК-1-1. Знает принципы сбора, отбора и обобщения информации	Теоретическая и практическая значимость	В работе использованы новые современные математические, естественнонаучные и другие методы профессиональной деятельности	В работе использованы стандартные современные математические, естественнонаучные и другие методы профессиональной деятельности	В работе использованы стандартные математические, естественнонаучные и другие методы профессиональной деятельности, известные достаточно длительное время	В работе использованы устаревшие математические, естественнонаучные и другие методы профессиональной деятельности
	ИУК-1-2. Умеет соотносить разнородные явления и систематизировать их в рамках избранных видов профессиональной деятельности		В работе предлагается новый алгоритм (методика) решения профессиональной задачи, имеющий теоретическую и/или практическую значимость	В работе предлагается новый алгоритм (методика) решения профессиональной задачи, имеющий теоретическую и/или практическую значимость, но имеющий много аналогов	В работе предлагается новый алгоритм (методика) решения профессиональной задачи, базирующийся на незначительных модификациях известных методик	В работе не предлагается новых алгоритмов (методик) решения профессиональной задачи
	ИУК-1-3. Имеет практический опыт работы с информационными объектами и сетью Интернет, опыт научного поиска, опыт библиографического разыскания, создания научных текстов		В работе предлагается новый алгоритм (методика) решения профессиональной задачи, имеющий теоретическую и/или практическую значимость	В работе предлагается новый алгоритм (методика) решения профессиональной задачи, имеющий теоретическую и/или практическую значимость, но имеющий много аналогов	В работе предлагается новый алгоритм (методика) решения профессиональной задачи, базирующийся на незначительных модификациях известных методик	В работе не предлагается новых алгоритмов (методик) решения профессиональной задачи
УК-2: Способен управлять проектом на всех этапах его жизненного цикла	ИУК-2.1. Знать: методы управления проектами; этапы жизненного цикла проекта	Теоретическая и практическая значимость	В работе подробно изложена методика получения экспериментальных данных, методика проведения теоретических расчё-	В работе изложена общая методика получения экспериментальных данных, общая методика проведения теоретических	В работе слабо освещена методика получения экспериментальных данных, методика проведения теоретических расчётов и моде-	Продемонстрирован недостаточный уровень проработки теоретических моделей и экспериментальных ре-

			тов и моделирования	расчётов и моделирования;	лирования	зультатов
	ИУК-2.2. Уметь: разрабатывать и анализировать альтернативные варианты проектов для достижения намеченных результатов; разрабатывать проекты, определять целевые этапы и основные направления работ		- обоснована состоятельность применения использованного оборудования и средств проведения теоретических расчётов/моделирования; - в работе представлена исчерпывающая физико-математическая модель рассматриваемых процессов, явлений и систем.	- частично обоснована состоятельность применения использованного оборудования и средств проведения теоретических расчётов/моделирования; - в работе представлена физико-математическая модель рассматриваемых процессов, явлений и систем.	- отсутствует теоретическая интерпретация экспериментальных данных; - не обоснована адекватность используемых теоретических моделей и корректность используемых экспериментальных методов;	Продemonстрирован недостаточный уровень проработки теоретических моделей и экспериментальных результатов
	ИУК-2.3. Иметь практический опыт: разработки проектов в избранной профессиональной сфере; методами оценки эффективности проекта, а также потребности в ресурсах		- все экспериментальные данные имеют теоретическую интерпретацию; - доказана адекватность используемых теоретических моделей и корректность используемых экспериментальных методов;	- экспериментальные данные имеют лишь частичную теоретическую интерпретацию; - адекватность используемых теоретических моделей и корректность используемых экспериментальных методов обоснована частично;	- не обоснована состоятельность применения использованного оборудования и средств проведения теоретических расчётов/моделирования; - в работе не представлена цельная физико-математическая модель рассматриваемых процессов, явлений и систем.	Продemonстрирован недостаточный уровень проработки теоретических моделей и экспериментальных результатов
УК-3: Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	ИУК-3.1. Знать методики формирования команд; методы эффективного руководства коллективами.	Теоретическая и практическая значимость	Работа свидетельствует о слаженной работе совместно с руководителем, самостоятельном определении траектории развития проекта и управления им	Работа свидетельствует о слаженной работе совместно с руководителем, но недостаточно самостоятельном определении траектории развития проекта и управления им	Работа свидетельствует о том, что не все задачи, поставленные научным руководителем, удалось выполнить в полном объеме	Работа не продемонстрировала навыков командной работы, умения слушать мнение руководителя и определять самостоятельную стратегию развития проекта

	ИУК-3.2. Уметь разрабатывать командную стратегию; организовывать работу коллективов; управлять коллективом; разрабатывать мероприятия по личностному, образовательному и профессиональному росту.		Работа свидетельствует о слаженной работе совместно с руководителем, самостоятельном определении траектории развития проекта и управления им	Работа свидетельствует о слаженной работе совместно с руководителем, но недостаточно самостоятельном определении траектории развития проекта и управления им	Работа свидетельствует о том, что не все задачи, поставленные научным руководителем, удалось выполнить в полном объеме	Работа не продемонстрировала навыков командной работы, умения слушать мнение руководителя и определять самостоятельную стратегию развития проекта
	ИУК-3.3. Владеть методами организации и управления коллективом, планированием его действий.		Работа свидетельствует о слаженной работе совместно с руководителем, самостоятельном определении траектории развития проекта и управления им	Работа свидетельствует о слаженной работе совместно с руководителем, но недостаточно самостоятельном определении траектории развития проекта и управления им	Работа свидетельствует о том, что не все задачи, поставленные научным руководителем, удалось выполнить в полном объеме	Работа не продемонстрировала навыков командной работы, умения слушать мнение руководителя и определять самостоятельную стратегию развития проекта
УК-4: Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	ИУК-4.1. Знать современные коммуникативные технологии на государственном и иностранном языках; закономерности деловой устной и письменной коммуникации.	Структура выступления	Построение грамотного и системного с точки зрения профессиональной коммуникации выступления на защите ВКР	Построение грамотного и преимущественно системного с точки зрения профессиональной коммуникации выступления на защите ВКР	Построение грамотного, но недостаточно системного с точки зрения профессиональной коммуникации, выступления на защите ВКР	
	ИУК-4.2. Уметь применять на практике коммуникативные технологии, методы и способы делового общения.		Структура выступления полностью соответствует требованиям	Структура выступления соответствует большинству требований	Структура выступления соответствует большинству требований, имеются нарушения временного регламента	

	ИУК-4.3. Владеть методикой межличностного делового общения на государственном и иностранном языках, с применением профессиональных языковых форм и средств.		Структура выступления учитывает требования доступности, акцентированности и наглядности изложения	Структура выступления учитывает требования доступности, акцентированности и наглядности изложения, но имеются незначительные замечания	Структура выступления учитывает требования доступности, акцентированности и наглядности изложения, но имеются существенные замечания	
УК-5: Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	ИУК-5.1. Знать сущность, разнообразие и особенности различных культур, их соотношение и взаимосвязь.	Корректность использованного инструментария	В работе прослеживаются полное обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты	В работе прослеживаются большинство этапов обоснования состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты	В работе прослеживаются некоторые этапы обоснования состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты	В работе не прослеживается большинство этапов обоснования состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты
	ИУК-5.2. Уметь обеспечивать и поддерживать взаимопонимание между представителями различных культур и навыки общения в мире культурного многообразия.		В работе имеется подробный анализ аналогичных альтернативных проектов	В работе имеется достаточный анализ аналогичных альтернативных проектов	В работе имеется поверхностный анализ аналогичных альтернативных проектов	В работе не приведен анализ аналогичных альтернативных проектов
	ИУК-5.3. Владеть способами анализа разногласий и конфликтов в межкультурной коммуникации и их разрешения.		В работе проведен подробный анализ эффективности разработанного обоснования состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты	В работе проведен достаточный анализ эффективности разработанного обоснования состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты	В работе проведен поверхностный анализ эффективности разработанного обоснования состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты	В работе не проведен анализ эффективности разработанного обоснования состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты

УК-6: Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки	ИУК-6.1. Знать основные принципы профессионального и личностного развития, исходя из этапов карьерного роста и требований рынка труда; способы совершенствования своей деятельности на основе самооценки.	Владение профессиональной терминологией	Работа написана в полном соответствии с нормами профессиональной коммуникации, адекватно использована профессиональная терминология	Работа написана в полном соответствии с нормами профессиональной коммуникации, адекватно использована профессиональная терминология в большинстве случаев	Работа написана в соответствии с нормами профессиональной коммуникации, имеется большое количество замечаний по адекватности использования профессиональной терминологии	Работа написана не в полном соответствии с нормами профессиональной коммуникации, не адекватно использована профессиональная терминология
	ИУК-6.2. Уметь решать задачи собственного профессионального и личностного развития, включая задачи изменения карьерной траектории; расставлять приоритеты.		В работе имеется подробное, системное, грамотное описание новых приобретенных знаний	В работе имеется достаточно системное и грамотное описание новых приобретенных знаний, но имеются некоторые замечания	В работе имеется описание новых приобретенных знаний, но оно в недостаточной степени удовлетворяет нормам профессиональной коммуникации	В работе имеется большое количество замечаний в части использования профессиональной терминологии при описании новых знаний
	ИУК-6.3. Владеть способами управления своей познавательной деятельностью и ее совершенствования на основе самооценки и принципов образования в течение всей жизни.		Приведено подробное и грамотное описание предлагаемого алгоритма (методики)	Приведено подробное и грамотное описание предлагаемого алгоритма (методики) с незначительными неточностями в применении профессиональной терминологии	Приведено описание предлагаемого алгоритма (методики), в целом, соответствующее профессиональной терминологии, но с существенными замечаниями	Описание предлагаемого алгоритма имеет существенные недостатки в части использования профессиональной терминологии
ОПК-1: Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	ИОПК-1.1. Знать: основные требования к системе обеспечения информационной безопасности и уметь разрабатывать проект технического задания на ее создание	Владение профессиональной терминологией	Управление проектом описано в корректном профессиональном стиле	Управление проектом описано в корректном профессиональном стиле с незначительными замечаниями	Управление проектом описано в корректном профессиональном стиле с существенными замечаниями	Управление проектом описано некорректно с точки зрения профессионального стиля

	ИОПК-1.2. Уметь: уметь применять основные и профессиональные обороты русского и иностранного языка при формулировке и доказательстве научных результатов		Сравнительный анализ технологий разработки проектов организационно-распорядительных документов выполнен в корректном профессиональном стиле	Сравнительный анализ технологий разработки проектов организационно-распорядительных документов выполнен в корректном профессиональном стиле с незначительными замечаниями	Сравнительный анализ технологий разработки проектов организационно-распорядительных документов выполнен в корректном профессиональном стиле с существенными замечаниями	Сравнительный анализ технологий разработки проектов организационно-распорядительных документов выполнен в некорректно с точки зрения профессионального стиля
	ИОПК-1.3. Владеть: основными и профессиональными устными и письменными оборотами русского и иностранного языков при формулировке и доказательстве научных результатов		Описание использования разработанного приложения выполнено в корректном профессиональном стиле	Описание использования разработанного приложения выполнено в корректном профессиональном стиле с незначительными замечаниями	Описание использования разработанного приложения выполнено в корректном профессиональном стиле с существенными замечаниями	Описание использования разработанного приложения выполнено в некорректно с точки зрения профессионального стиля
ОПК-2: Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности	ИОПК-2.1. Знать: основные понятия и принципы делопроизводства и электронного документооборота; основные стандарты в области инфокоммуникационных систем и технологий; основные отечественные и зарубежные стандарты в области компьютерной безопасности; методологические основы теории принятия решений, теории изменений, теории прогнозирования и планирования; способы измерения свойств объек-	Владение профессиональной терминологией	При разработке алгоритма использовались современные научные принципы и методы исследований в области информационной безопасности	При разработке алгоритма использовались популярные, но давно известные, научные принципы и методы исследований в области информационной безопасности	При разработке алгоритма использовались устаревшие научные принципы и методы исследований в области информационной безопасности	

	<p>тов предметной области; методы оценки эффективности и качества в задачах прогнозирования, планирования, принятия решений при различной априорной неопределенности имеющейся информации; основные типы статистических задач и математические методы их решения; основные математические методы исследования случайных процессов; основные теоретико-числовые методы применительно к задачам защиты информации; физические основы функционирования технических средств и систем обработки и передачи информации; физические основы образования технических каналов утечки информации; основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; методы концептуального проектирования технологий обеспечения информации</p>					
--	---	--	--	--	--	--

	онной безопасности.					
	<p>ИОПК-2.2. Уметь: классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; готовить проекты нормативно-распорядительных документов (приказов, указаний, инструкций); готовить проектную документацию на создаваемые специальные АИС; разрабатывать частные политики безопасности компьютерных систем, в том числе, политики управления доступом и информационными потоками; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования; использовать результаты научно-исследовательских работ в решении задач практики; использовать современные мо-</p>		<p>При разработке алгоритма использовались современные научные принципы и методы исследований в области информационной безопасности</p>	<p>При разработке алгоритма использовались популярные, но давно известные, научные принципы и методы исследований в области информационной безопасности</p>	<p>При разработке алгоритма использовались устаревшие научные принципы и методы исследований в области информационной безопасности</p>	

	<p>дели и методы измерения, прогнозирования, планирования, принятия решений при решении практических задач; самостоятельно строить вероятностные модели применительно к практическим задачам и производить статистическую оценку адекватности полученной модели и реальных задач; применять теоретикочисловые методы для оценки криптографических свойств систем защиты информации; применять системы компьютерной математики для решения типовых задач; использовать физические эффекты для обеспечения технической защиты информации; осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; организовывать работы по совер-</p>					
--	--	--	--	--	--	--

	шенствованию, модернизации и унификации технологий обеспечения информационной безопасности					
	ИОПК-2.3. Владеть: основной юридической терминологией, используемой в гражданском, гражданско-процессуальном, административном, уголовном, уголовно-процессуальном и финансовом законодательстве; навыками письменного аргументированного изложения собственной точки зрения; навыками публичной речи, аргументации, ведения дискуссии и полемики; навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности; основными методами научного познания; навыками использования стандартных методов и моделей математического анализа и их применения к решению прикладных задач; навыками ана-		При разработке алгоритма использовались современные научные принципы и методы исследований в области информационной безопасности	При разработке алгоритма использовались популярные, но давно известные, научные принципы и методы исследований в области информационной безопасности	При разработке алгоритма использовались устаревшие научные принципы и методы исследований в области информационной безопасности	

	литического и численного решения задач математической статистики; методами проведения физического эксперимента при выявлении технических каналов утечки информации					
ОПК-3: Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности	ИОПК-3.1. Знать: основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; методы концептуального проектирования технологий обеспечения информационной безопасности; основные нормативные правовые акты в области информационной безопасности и защиты информации; основные понятия, законы, модели и структуры обеспечения организационной безопасности на предприятии; основные понятия, законы и модели прогнозирования принятия решений	Использование нормативных документов в области ИБ	Требования нормативных документов в области ИБ соблюдены в полном объеме	Имеются незначительные нарушения нормативных требований.	Имеются систематические нарушения нормативных требований.	Продemonстрирована неспособность соблюдать нормативных требований
	ИОПК-3.2. Уметь: - осуществлять выбор		Требования нормативных документов в области ИБ соблюдены в	Имеются незначительные нарушения нормативных требований.	Имеются систематические нарушения нормативных требований.	Продemonстрирована неспособность соблюдать норма-

	<p>функциональной структуры системы обеспечения информационной безопасности; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности; использовать нормативные правовые документы в своей профессиональной деятельности; применять основные закономерности принятия управленческих решений и управления коллективом при решении прикладных задач обеспечения информационной безопасности</p>		полном объёме			тивных требований
	<p>ИОПК-3.3. Владеть: навыками управления информационной безопасностью простых объектов; навыками освоения, внедрения и сопровождения документации, в том числе и в команде;</p>		Требования нормативных документов в области ИБ соблюдены в полном объёме	Имеются незначительные нарушения нормативных требований.	Имеются систематические нарушения нормативных требований.	Продemonстрирована неспособность соблюдать нормативных требований

	<p>навыками нахождения организационно-управленческих решений в нестандартных ситуациях на основе результатов анализа документации и потоков документов; знаниями в области правового обеспечения информационной безопасности и навыками правоприменения нормативного законодательства в данной сфере; навыками поиска нормативной и технической информации, необходимой для профессиональной деятельности, обоснования, выбора, реализации и контроля результатов работы</p>					
<p>ОПК-4: Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок</p>	<p>ИОПК-4.1. Знать: основные категории и понятия информационно-аналитической работы, принципы и методы ее ведения; источники специальной информации; методы оценивания ее достоверности; виды информационных моделей и способы их построения; методы накопления специальной информации; ме-</p>	<p>Литературный обзор</p>	<p>- В теоретической части работы представлен достаточно полный литературный обзор по рассматриваемой проблеме;</p>	<p>- В теоретической части работы представлен недостаточно полный литературный обзор по рассматриваемой проблеме;</p>	<p>- В теоретической части работы не представлен литературный обзор по рассматриваемой проблеме;</p>	<p>- В теоретической части работы не представлен литературный обзор по рассматриваемой проблеме;</p>

	тоды подготовки специальной информации; методы выработки и принятия информационного решения; виды отчетно-информационных документов, методы их подготовки; основные математические методы исследования случайных процессов; основные теоретико-числовые методы применительно к задачам защиты информации; физические основы функционирования технических средств и систем обработки и передачи информации; физические основы образования технических каналов утечки информации; методы концептуального проектирования технологий обеспечения информационной безопасности.					
	ИОПК-4.2. Уметь: использовать руководящие, нормативные и методические документы по организации информационно-аналитической работы; - использовать справочную и научную	- в практической части работы представлены ссылки на смежные источники информации либо релевантными результатами;	- в практической части работы практически не представлены либо отсутствуют ссылки на смежные источники информации с аналогичными либо релевантными результатами;	- в практической части работы отсутствуют ссылки на смежные источники информации либо релевантными результатами;	- в практической части работы отсутствуют ссылки на смежные источники информации либо релевантными результатами;	

	<p>литературу по тематике решаемых информационных задач; оценивать специальную информацию, систематизировать ее, принимать решения о ее дальнейшем использовании; разрабатывать основные виды отчетно-информационных документов; применять средства автоматизации информационно-аналитической работы; использовать разнообразные источники сведений, отчетно-информационные документы добывающих органов различных видов, в том числе на иностранном языке; применять теоретико-числовые методы для оценки криптографических свойств систем защиты информации; применять системы компьютерной математики для решения типовых задач; использовать физические эффекты для обеспечения технической защиты информации; применять на практике методы физики при исследовании техни-</p>					
--	--	--	--	--	--	--

	ческих каналов утечки информации; осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности.					
	ИОПК-4.3. Владеть: Основными системными подходами к определению целей, задач информационно-аналитической работы и источников специальной информации; информацией о современных и перспективных системах автоматизации информационно-аналитической работы; навыками аналитического и численного решения задач математической статистики; методами проведения физического		- список литературы содержит не менее 20 библиографических наименований, относящихся к рецензируемым источникам информации.	- список литературы содержит не менее 10 библиографических наименований, относящихся к рецензируемым источникам информации	- список литературы содержит не менее 5 библиографических наименований, относящихся к рецензируемым источникам информации	- список литературы содержит менее 5 библиографических наименований, относящихся к рецензируемым источникам информации.

	эксперимента при выявлении технических каналов утечки информации.					
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.	ИОПК-5.1. Знать: основные классификационные признаки экспериментов; основные элементы научно-технического эксперимента; приемы выбора основных факторов эксперимента и технологию построения факторных планов, основные виды регрессионных экспериментов, основные типы оптимальных экспериментов; основные типы статистических задач и математические методы их решения; основные математические методы исследования случайных процессов; основные теоретико-числовые методы применительно к задачам защиты информации; физические основы функционирования технических средств и систем обработки и передачи информации;	Владение профессиональной терминологией	В работе использовались новые современные интеллектуальные технологии обработки результатов эксперимента	В работе использовались известные современные интеллектуальные технологии обработки результатов эксперимента	В работе использовались популярные, но давно известные, интеллектуальные технологии обработки результатов эксперимента	В работе не использовались интеллектуальные технологии обработки результатов эксперимента

	физические основы образования технических каналов утечки информации; основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; методы концептуального проектирования технологий обеспечения информационной безопасности..					
	ИОПК-5.2. Уметь: проводить классификацию экспериментов; выбирать необходимые факторы и составлять факторные планы экспериментов различного вида; строить системы базисных функций, делать точечные оценки параметров регрессионной модели; анализировать свойства оценок параметров регрессионной модели; выполнять оптимальное планирование экспериментов с использованием различных критериев; самостоятельно строить вероятностные модели применительно к практическим зада-		В работе приведено подробное обоснование выбора соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента	В работе приведено достаточное обоснование выбора соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента	В работе приведено поверхностное обоснование выбора соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента	В работе не приведено обоснование выбора соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента

	<p>чам и производить статистическую оценку адекватности полученной модели и реальных задач; применять теоретико-числовые методы для оценки криптографических свойств систем защиты информации; применять системы компьютерной математики для решения типовых задач; использовать физические эффекты для обеспечения технической защиты информации; осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности</p>					
--	--	--	--	--	--	--

	ИОПК-5.3. Владеть: методами выбора основных факторов эксперимента; методами подбора эмпирических зависимостей для экспериментальных данных; методами оценки коэффициентов регрессионной модели эксперимента; методами построения оптимальных планов для научных экспериментов; навыками аналитического и численного решения задач; методами проведения физического эксперимента при выявлении технических каналов утечки информации		В работе предлагается новая методика экспериментальных исследований защищенности объектов, имеющая теоретическую и/или практическую значимость	В работе предлагается новая методика экспериментальных исследований защищенности объектов, имеющая теоретическую и/или практическую значимость, но имеющая много аналогов	В работе предлагается новая методика экспериментальных исследований защищенности объектов, имеющая теоретическую и/или практическую значимость, базирующаяся на незначительных модификациях известных методик	В работе не предлагается новых методик экспериментальных исследований защищенности объектов
ПК-1: Способность анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты	ИПК-1.1. Знать: основные теоретико-числовые методы применительно к задачам защиты информации; физические основы функционирования технических средств и систем обработки и передачи информации; физические основы образования технических каналов утечки информации; основные принципы организации технического, программного и ин-	Владение профессиональной терминологией	Приведен анализ актуальности темы	Приведенный анализ актуальности темы не содержит достаточного количества аргументов	Приведенный анализ актуальности темы базируется на устаревшей информации и не полностью достоверен	Тема работы устаревшая, работа не содержит анализа актуальности темы

	формационного обеспечения защищенных информационных систем; методы концептуального проектирования технологий обеспечения информационной безопасности					
	ИПК-1.2. уметь: самостоятельно строить вероятностные модели применительно к практическим задачам и производить статистическую оценку адекватности полученной модели и реальных задач; применять теоретико-числовые методы для оценки криптографических свойств систем защиты информации; применять системы компьютерной математики для решения типовых задач; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной		Анализ актуальности темы базируется на большом количестве аргументов, обосновывающих выбор используемых задач и методов	Анализ актуальности темы базируется на достаточном количестве аргументов, обосновывающих выбор используемых задач и методов, но некоторые не являются достаточно убедительными	Анализ актуальности темы имеется, но базируется на недостаточном количестве аргументов	Анализ актуальности темы не приведен

	безопасности.					
	ИПК-1.3. владеть: навыками аналитического и численного решения задач математической статистики; методами проведения физического эксперимента при выявлении технических каналов утечки информации; навыками управления информационной безопасностью простых объектов.					
ПК-2: Способность проводить аудит информационной безопасности информационных систем и объектов информатизации	ИПК-2.1. Знать: суть методологии и методы научного познания, методы анализа информационных процессов и систем, средства структурного анализа, математические модели информационных процессов; основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; методы концептуального проектирования техноло-	Владение профессиональной терминологией	Используемые методы проведения аудита содержат научную новизну и показывают эффективность их применения	Используемые методы проведения аудита указывают на перспективы получения научной новизны и показывают эффективность их применения	Используемые методы проведения аудита не содержат научную новизну, но демонстрируют стремление к ее получению	Используемые методы проведения аудита не содержат научную новизну и не демонстрируют стремление к ее получению

	гий обеспечения информационной безопасности.					
	ИПК-2.2. Уметь: ставить и решать типовые задачи в области структурного анализа информационных процессов и систем, разрабатывать модели предметных областей, проводить исследования характеристик компонентов информационных процессов и информационных систем в целом; осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности		Полученные результаты (алгоритм, методика, проведенный эксперимент) демонстрируют умение планировать и управлять ходом научного исследования и разработки программного обеспечения	Полученные результаты (алгоритм, методика, проведенный эксперимент) демонстрируют умение планировать и управлять ходом научного исследования и разработки программного обеспечения в достаточной степени	Полученные результаты (алгоритм, методика, проведенный эксперимент) демонстрируют умение планировать и управлять ходом научного исследования и разработки программного обеспечения с существенными недостатками	Полученные результаты (алгоритм, методика, проведенный эксперимент) не демонстрируют умение планировать и управлять ходом научного исследования и разработки программного обеспечения
	ИПК-2.3. Владеть: методами анализа информационных про-		Полученные результаты (алгоритм, методика, проведенный эксперимент) демонстри-	Полученные результаты (алгоритм, методика, проведенный эксперимент) демонстри-	Полученные результаты (алгоритм, методика, проведенный эксперимент) демонстри-	Полученные результаты (алгоритм, методика, проведенный экс-

	цессов и систем, методами разработки математических моделей информационных процессов; навыками управления информационной безопасностью простых объектов		руют умение планировать и управлять информационной безопасностью простых объектов	руют умение планировать и управлять информационной безопасностью простых объектов в достаточной степени	руют умение планировать и управлять информационной безопасностью простых объектов с существенными недостатками	перимент) не демонстрируют умение планировать и управлять ходом информационной безопасностью простых объектов
ПК-3: Способность проводить аттестацию объектов информатизации по требованиям безопасности информации	ИПК-3.1. Знать: - основные принципы обеспечения информационной безопасности и защиты информации; структуру систем документационного обеспечения; - основные понятия и методы в области управления службой безопасности предприятия; организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации; основные нормативные правовые акты в области обеспечения информационной	Корректность использованного инструментария	В работе прослеживаются полное обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты	В работе прослеживаются большинство этапов обоснования состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты	В работе прослеживаются некоторые этапы обоснования состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты	В работе не прослеживается большинство этапов обоснования состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты

	<p>безопасности и нормативные методические документы ФСБ России и ФСТЭК России. Знать понятия и виды защищаемой информации; виды основных угроз защищаемой информации; базовые понятия о методах и средствах защиты информации; международные стандарты информационной безопасности</p>					
	<p>ИПК-3.2. Уметь: - анализировать и оценивать угрозы информационной безопасности объекта; - пользоваться нормативными документами по защите информации; - определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; - определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности сведений, составляющих государственную и коммерческую тайну;</p>					
			<p>В работе имеется подробный анализ аналогичных альтернативных проектов</p>	<p>В работе имеется достаточный анализ аналогичных альтернативных проектов</p>	<p>В работе имеется поверхностный анализ аналогичных альтернативных проектов</p>	<p>В работе не приведен анализ аналогичных альтернативных проектов</p>

	<p>уметь проводить процедуры аттестации, категорирования объектов информатизации; уметь пользоваться научно-технической и справочной литературой для решения прикладных задач; осуществлять поиск информации в Интернет и выполнять аналитического исследования по определенной теме.</p>					
	<p>ИПК-3.3. Владеть: навыками анализа методов и средств передачи, хранения и обработки данных, навыками применения средств охраны от негативных воздействий, навыками оценки защищенности объектов информатизации, навыками организации охраны на объектах информатизации, навыками применения технических средств защиты информации; - типовыми приемами проектирования, инструментарием для документирования проектных решений, методами прямого и обратного проектирова-</p>		<p>В работе проведен подробный анализ эффективности разработанного обоснования состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты</p>	<p>В работе проведен достаточный анализ эффективности разработанного обоснования состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты</p>	<p>В работе проведен поверхностный анализ эффективности разработанного обоснования состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты</p>	<p>В работе не проведен анализ эффективности разработанного обоснования состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты</p>

	<p> ния; :- навыками анализа информационной инфраструктуры информационной системы и ее безопасности; пользоваться нормативными документами по противодействию технической разведке; применять действующую законодательную базу в области обеспечения информационной безопасности; применять нормативные правовые акты и нормативные методические документы в области обеспечения безопасности сведений, составляющих государственную и коммерческую тайну; владеть методами и средствами защиты информации, применяемыми в деятельности службы безопасности на предприятиях для обеспечения защиты сведений, составляющих государственную и коммерческую тайну </p>					
--	---	--	--	--	--	--

ПК-4: Способность создания педагогических условий для развития группы обучающихся по программам ВО, организационно-методическое, преподавание для программ бакалавриата, ориентированным на соответствующий уровень квалификации	ИПК-4.1 Знает педагогические условия для развития группы обучающихся по программам ВО, организационно-методическое сопровождение, преподавание для программ бакалавриата, ориентированным на соответствующий уровень квалификации	Качество ответов на вопросы	Стиль ответов на вопросы учитывает требования доступности и наглядности	Стиль ответов на вопросы учитывает требования доступности и наглядности с незначительными замечаниями	Стиль ответов на вопросы учитывает требования доступности и наглядности с существенными замечаниями	Стиль ответов на вопросы не учитывает требования доступности и наглядности
	ИПК-4.2 Умеет создавать педагогические условия для развития группы обучающихся по программам ВО, организационно-методическое сопровождение, преподавание для программ бакалавриата, ориентированным на соответствующий уровень квалификации		Стиль ответов на вопросы учитывает требования доступности и наглядности	Стиль ответов на вопросы учитывает требования доступности и наглядности с незначительными замечаниями	Стиль ответов на вопросы учитывает требования доступности и наглядности с существенными замечаниями	Стиль ответов на вопросы не учитывает требования доступности и наглядности
	ИПК-4.3 Имеет практический опыт создания педагогических условий для развития группы обучающихся по программам ВО, организационно-методического сопровождения, преподавания для программ бакалавриата, ориентированным на соответ-		Стиль ответов на вопросы учитывает требования доступности и наглядности	Стиль ответов на вопросы учитывает требования доступности и наглядности с незначительными замечаниями	Стиль ответов на вопросы учитывает требования доступности и наглядности с существенными замечаниями	Стиль ответов на вопросы не учитывает требования доступности и наглядности

	ствующий уровень квалификации					
ПК-5: Способность организовать управление информационной безопасностью	ИПК-5.1. Знать: – разновидности и свойства систем управления; - основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области; технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации; - принципы и методы организационной защиты информации, создания систем охранно-тревожной сигнализации, систем контроля и управления доступом, охранного телевидения; - принципы и методы проти-	Корректность использованного инструментария	Реализованы все этапы жизненного цикла разработки проекта	Реализованы большинство этапов жизненного цикла разработки проекта	Реализованы некоторые этапы жизненного цикла разработки проекта, но, в целом, проект состоялся	Не реализованы большинство этапов жизненного цикла разработки проекта, в результате чего проект потерял целостность

	<p> воздействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации; - методологию организационной защиты информации, ее современные проблемы и терминологию; - основные руководящие документы по обеспечению режима и секретности на объекте; - типовую структуру службы безопасности, ее основные задачи и функции должностных лиц; - основные документы, регламентирующие организационную безопасность на объекте; - правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны; - правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации; - основные принципы организации технического, </p>					
--	--	--	--	--	--	--

	программного и информационного обеспечения защищенных информационных систем					
	ИПК-5.2. Уметь: – программно реализовывать алгоритмы управления в цифровых системах; - применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем; - пользоваться нормативными документами по защите информации; - оценивать состояние организационной защиты информации на объекте; - определять рациональные меры по обеспечению организационной защите на объекте; - организовать работу с персоналом с секретной (конфиденциальной) информацией; - формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, администра-		В работе прослеживается самостоятельно разработанная траектория управления информационной безопасностью	В работе прослеживается преимущественно самостоятельно разработанная траектория управления информационной безопасностью	Траектория управления информационной безопасностью разработана и реализована научным руководителем	Не прослеживается траектория управления информационной безопасностью

	тивно-управленческой и технической реализуемости; - самостоятельно осуществлять изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности					
	ИПК-5.3. Владеть: - навыками работы с нормативными правовыми актами; - профессиональной терминологией; навыками формирования методических и нормативных документов, тех. документации в области обеспечения информационной безопасности; знаниями в области правового обеспечения информационной безопасности и навыками правоприменения нормативного законодательства в данной сфере; - навыками поиска норма-		В работе прослеживается самостоятельно разработанная траектория управления информационной безопасностью	В работе прослеживается преимущественно самостоятельно разработанная траектория управления информационной безопасностью	Траектория управления информационной безопасностью разработана и реализована научным руководителем	Не прослеживается траектория управления информационной безопасностью

	<p>тивной и технической информации, необходимой для профессиональной деятельности, обоснования, выбора, реализации и контроля результатов работы; навыками управления информационной безопасностью простых объектов; – методами анализа и синтеза систем управления; – навыками использования микропроцессоров и микроЭВМ в системах управления</p>					
<p>ПК-6: Способен обобщать и критически оценивать опыт и результаты научных исследований в области информационной безопасности</p>	<p>ИПК-6.1. Знать: основные понятия и принципы делопроизводства и электронного документооборота; основные стандарты в области инфокоммуникационных систем и технологий; основные отечественные и зарубежные стандарты в области компьютерной безопасности; методологические основы теории принятия решений, теории измерений, теории прогнозирования и планирования; способы измерения свойств объектов предметной области</p>		<p>В работе приведено подробное описание предлагаемой методики</p>	<p>В работе приведено достаточное описание предлагаемой методики</p>	<p>В работе приведено поверхностное описание предлагаемой методики</p>	<p>Описание предлагаемой методики содержит большое количество недостатков</p>

	<p>ти; методы оценки эффективности и качества в задачах прогнозирования, планирования, принятия решений при различной априорной неопределенности имеющейся информации; основные типы статистических задач и математические методы их решения; основные математические методы исследования случайных процессов; основные теоретико-числовые методы применительно к задачам защиты информации; физические основы функционирования технических средств и систем обработки и передачи информации; физические основы образования технических каналов утечки информации; основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; методы концептуального проектирования технологий обеспечения информации-</p>					
--	--	--	--	--	--	--

	онной безопасности.					
	ИПК-6.2. Уметь: классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; готовить проекты нормативно-распорядительных документов (приказов, указаний, инструкций); готовить проектную документацию на создаваемые специальные АИС; разрабатывать частные политики безопасности компьютерных систем, в том числе, политики управления доступом и информационными потоками; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования; использовать результаты научно-исследовательских работ в решении задач практики; использовать современные мо-		В работе содержится подробный аналитический обзор литературы	В работе содержится достаточный аналитический обзор литературы	В работе содержится поверхностный аналитический обзор литературы	Аналитический обзор литературы содержит большое количество недостатков

	<p>дели и методы измерения, прогнозирования, планирования, принятия решений при решении практических задач; самостоятельно строить вероятностные модели применительно к практическим задачам и производить статистическую оценку адекватности полученной модели и реальных задач; применять теоретикочисловые методы для оценки криптографических свойств систем защиты информации; применять системы компьютерной математики для решения типовых задач; использовать физические эффекты для обеспечения технической защиты информации; осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; организовы-</p>					
--	--	--	--	--	--	--

	<p>вать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности</p>					
	<p>ИПК-6.3. Владеть: основной юридической терминологией, используемой в гражданском, гражданско-процессуальном, административном, уголовном, уголовно-процессуальном и финансовом законодательстве; навыками письменного аргументированного изложения собственной точки зрения; навыками публичной речи, аргументации, ведения дискуссии и полемики; навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности; основными методами научного познания; навыками использования стандартных методов и моделей математического анализа и их применения к решению прикладных задач; навыками ана-</p>		<p>В работе содержится подробное обоснование выбранных методик решения задачи</p>	<p>В работе содержится достаточное обоснование выбранных методик решения задачи</p>	<p>В работе содержится поверхностное обоснование выбранных методик решения задачи</p>	<p>Обоснование выбранных методик решения задачи содержит большое количество недостатков</p>

	литического и числен-ного решения задач математической статисти-ки; методами про-ведения физического эксперимента при вы-явлении технических каналов утечки ин-формации					
--	---	--	--	--	--	--

4.4. Примерные темы выпускных квалификационных работ

1. Разработка аппаратного токена на микроконтроллере STM32F103C8T6 для организации защищенного хранения данных
2. Аудит системной безопасности ОС Linux
3. Аудит информационной безопасности устройств на основе ОС Android
4. Аутентификация пользователей на основе RADIUS-сервера
5. Анализ сообщений по заданной тематике или автору для выявления автоматических комментариев в социальных сетях
6. Анализ данных, хранимых в реестрах криптовалют: классификация и профилирование участников, география сети
7. Разработка алгоритма скрытной передачи информации по коротковолновому радиоканалу
8. Защищенный канал связи на основе нейросетевой системы распределения криптографических ключей
9. Разработка макета речевого скремблера для телефонной линии связи с частотной инверсией сигнала
10. Разработка макета речевого скремблера для гражданской УКВ связи с перестановкой частотных поддиапазонов
11. Разработка программных средств защиты авторских прав программного обеспечения с использованием цифровых водяных знаков
12. Защищенный канал связи на основе нейросетевой системы распределения криптографических ключей
13. Исследование уязвимости БЛА по навигационным протоколам
14. Методы распознавания печатного и рукописного текста для задач идентификации
15. Методы распознавания изображений для задачи идентификации
16. Методы распознавания голоса для задач идентификации и аутентификации
17. Разработка комплекса контроля физического доступа на основе алгоритма KeeLog
18. Методы обнаружения утечки информации по акустическому каналу
19. Технические методы защиты информации от утечки по акустическому каналу
20. Коррекция статистических характеристик ключей шифрования с помощью математических экстракторов случайности
21. Реализация на уровне инструкций шифрования DES системы шифрации/дешифрации потока данных для микроконтроллера AVR XMEGA

Формулировки тем ВКР могут корректироваться в соответствии с индивидуальными возможностями, потребностями и траекториями обучения конкретных обучающихся, предложениями самих обучающихся, теоретической и практической актуальностью научных и научно-практических проблем.

**Приложение к протоколу
заседания ГЭК от _____ № _____**

Оценочный лист по подготовке к сдаче и сдаче выпускной квалификационной работы

ФИО обучающегося _____

Шифр Направление (профиль) _____

Группа _____

1. Общая характеристика текста выпускной квалификационной работы и защиты выпускной квалификационной работы обучающегося (в том числе отзывы и рецензии)

2. Вопросы, заданные обучающемуся:

3. Характеристика ответов обучающегося

4. Критерии оценивания освоения компетенций при подготовке к процедуре защиты и защиты выпускной квалификационной работы

Код компетенции	Расшифровка компетенции	Уровень освоения компетенции (подчеркнуть нужное)
УК-1	Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	Высокий Средний Низкий Ниже порогового
УК-2	Способен управлять проектом на всех этапах его жизненного цикла	Высокий Средний Низкий Ниже порогового
УК-3	Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	Высокий Средний Низкий Ниже порогового
УК-4	Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	Высокий Средний Низкий Ниже порогового
УК-5	Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	Высокий Средний Низкий Ниже порогового
УК-6	Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки	Высокий Средний Низкий Ниже порогового
ОПК-1	Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	Высокий Средний Низкий Ниже порогового
ОПК-2	Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности	Высокий Средний Низкий Ниже порогового
ОПК-3	Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности;	Высокий Средний Низкий Ниже порогового
ОПК-4	Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследова-	Высокий Средний

(подпись)

(Фамилия И.О.)

(подпись)

(Фамилия И.О.)

(подпись)

(Фамилия И.О.)

(подпись)

(Фамилия И.О.)

(подпись)

(Фамилия И.О.)

Секретарь ГЭК

(подпись)

(Фамилия И.О.)

Список литературы, необходимой для подготовки к процедуре защиты и защиты выпускной квалификационной работы

Направление подготовки / специальность: 10.04.01 Информационная безопасность
Направленность (профиль) подготовки Информационная безопасность автоматизированных систем
Квалификация выпускника: магистр
Форма обучения: очное
Язык обучения: русский
Год начала обучения по образовательной программе: 2023

Основная литература:

1. Кукушкина, В. В. Организация научно-исследовательской работы студентов (магистров): учебное пособие / В.В. Кукушкина. — Москва: ИНФРА-М, 2019. — 264 с. — (Высшее образование: Магистратура). - ISBN 978-5-16-101630-5. - Текст: электронный. - URL: <https://znanium.com/catalog/product/982657> (дата обращения: 10.06.2022). - Режим доступа: по подписке.
2. Космин, В. В. Основы научных исследований (Общий курс): учебное пособие / В.В. Космин. — 4-е изд., перераб. и доп. — Москва: РИОР: ИНФРА-М, 2019. — 238 с. — (Высшее образование). — DOI: <https://doi.org/10.12737/1753-1>. - ISBN 978-5-16-106389-7. - Текст: электронный. - URL: <https://znanium.com/catalog/product/1062101> (дата обращения: 10.03.2022). - Режим доступа: по подписке.
3. Пижурин, А. А. Методы и средства научных исследований: учебник / А.А. Пижурин, А.А. Пижурин (мл.), В.Е. Пятков. — Москва: ИНФРА-М, 2020. — 264 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-16-010816-2. - Текст: электронный. - URL: <https://znanium.com/catalog/product/1085368> (дата обращения: 10.03.2022). — Режим доступа: по подписке.
4. Курсовые и выпускные квалификационные работы. Методические рекомендации / Р.Н. Абайдуллин, А.А. Андрианова, Р.Ф. Хабибуллин. - Казань: Казанский университет, 2015. - 25 с. - Текст: электронный. - URL: http://dspace.kpfu.ru/xmlui/bitstream/net/20357/1/09_104_001108.pdf (дата обращения: 10.03.2022). — Режим доступа: открытый.
5. Марченков, С. С. Основы теории булевых функций: учебное пособие / С. С. Марченков. — Москва: ФИЗМАТЛИТ, 2014. — 136 с. — ISBN 978-5-9221-1562-9. — Текст: электронный // Лань: электронно-библиотечная система. — URL: <https://e.lanbook.com/book/59714> (дата обращения: 10.03.2022). — Режим доступа: для авториз. пользователей.
6. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах: учебное пособие / В.Ф. Шаньгин. — Москва: ИД «ФОРУМ»: ИНФРА-М, 2020. — 592 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-8199-0730-6. - Текст: электронный. - URL: <https://znanium.com/catalog/product/1093695> (дата обращения: 10.03.2022). — Режим доступа: по подписке.
7. Защита информации: учебное пособие / А. П. Жук, Е. П. Жук, О. М. Лепешкин, А. И. Тимошкин. - 3-е изд. - Москва: РИОР: ИНФРА-М, 2019. - 400 с. - (Высшее образование). - ISBN 978-5-369-01759-3. - Текст: электронный. - URL: <https://znanium.com/catalog/product/1018901> (дата обращения: 10.03.2022). — Режим доступа: по подписке.
8. Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками : учебное пособие для вузов / Девянин П. Н. - 2-е изд., испр. и доп. - Москва: Горячая линия - Телеком, 2013. - 338 с. - ISBN 978-5-9912-0328-9. - Текст: электронный // ЭБС "Консультант студента": [сайт]. - URL: <https://www.studentlibrary.ru/book/ISBN9785991203289.html> (дата обращения: 10.03.2022). - Режим доступа: по подписке.
9. Смолин, Ю.Н. Алгебра и теория чисел: учебное пособие / Ю.Н. Смолин. — 5-е изд., стер. — Москва: ФЛИНТА, 2017. — 464 с. - ISBN 978-5-9765-0050-1. - Текст: электронный. - URL: <https://znanium.com/catalog/product/1034573> (дата обращения: 10.03.2022). — Режим доступа: по подписке.
10. Основы комбинаторики и теории чисел. Сборник задач: учебное пособие / А. А. Глибичук, Д. Г. Ильинский, Д. В. Мусатов [и др.]. — 2-е изд. - Долгопрудный: Интеллект, 2019. - 104 с. - ISBN 978-5-91559-259-8. -

Текст: электронный. - URL: <https://znanium.com/catalog/product/1086282> (дата обращения: 10.03.2022). – Режим доступа: по подписке.

11. Чикрин, Д. Е. Теория информации и кодирования: курс лекций / Д. Е. Чикрин; Казан. (Приволж.) федер. ун-т, Высш. шк. информ. технологий и информ. систем, Каф. автоном. робототехн. систем. - Электронные данные (1 файл: 4,46 Мб). - (Казань: Казанский федеральный университет, 2013) - Текст: электронный. - URL: http://libweb.kpfu.ru/ebooks/50-ITIS/50_000337.pdf (дата обращения: 10.03.2022). – Режим доступа: по подписке.

12. Кнауб, Л. В. Теоретико-численные методы в криптографии: учебное пособие / Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов. - Красноярск: Сибирский федеральный университет, 2011. - 160 с. - ISBN 978-5-7638-2113-7. - Текст: электронный. - URL: <https://znanium.com/catalog/product/441493> (дата обращения: 10.03.2022). – Режим доступа: по подписке.

13. Федотов, И. Е. Модели параллельного программирования: практическое пособие / Федотов И.Е. - Москва: СОЛОН-Пресс, 2017. - 392 с. (Библиотека профессионала) ISBN 978-5-91359-222-4. - Текст : электронный. - URL: <https://znanium.com/catalog/product/858609> (дата обращения: 10.03.2022). – Режим доступа: по подписке.

Дополнительная литература:

1. Заботина, Н. Н. Проектирование информационных систем: учебное пособие / Н. Н. Заботина. — Москва: ИНФРА-М, 2020. — 331 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-16-004509-2. - Текст: электронный. - URL: <https://znanium.com/catalog/product/1036508> (дата обращения: 10.03.2022). – Режим доступа: по подписке.

2. Основы комбинаторики и теории чисел: учебное пособие / А. А. Глибичук, Д. Г. Ильинский, Д. В. Мусатов [и др.]. — 2-е изд. - Долгопрудный: Интеллект, 2019. - 104 с. - ISBN 978-5-91559-259-8. - Текст: электронный. - URL: <https://znanium.com/catalog/product/1086282> (дата обращения: 10.03.2022). – Режим доступа: по подписке.

3. Крылов, П.А. Упражнения по группам, кольцам и полям: учебное пособие / П.А. Крылов, А.А. Туганбаев, А.Р. Чехлов. — 2-е изд., стер. — Москва: ФЛИНТА, 2017. — 212 с. - ISBN 978-5-9765-1506-2. - Текст: электронный. - URL: <https://znanium.com/catalog/product/1034589> (дата обращения: 10.03.2022). – Режим доступа: по подписке.

4. Шоломов, Л. А. Основы теории дискретных логических и вычислительных устройств: учебное пособие / Л. А. Шоломов. — 3-е изд., испр. — Санкт-Петербург: Лань, 2011. — 432 с. — ISBN 978-5-8114-1197-9. — Текст: электронный // Лань: электронно-библиотечная система. — URL: <https://e.lanbook.com/book/1556> (дата обращения: 10.03.2022). — Режим доступа: для авториз. пользователей.

5. Применение искусственных нейронных сетей и системы остаточных классов в криптографии: монография / Н. И. Червяков, А. А. Евдокимов, А. И. Галушкин, И. Н. Лавриненко. — Москва: ФИЗМАТЛИТ, 2012. — 280 с. — ISBN 978-5-9221-1386-1. — Текст: электронный // Лань: электронно-библиотечная система. — URL: <https://e.lanbook.com/book/5300> (дата обращения: 10.03.2022). — Режим доступа: для авториз. пользователей.

Перечень информационных технологий, используемых для подготовки к процедуре защиты и защиты выпускной квалификационной работы, включая перечень программного обеспечения и информационных справочных систем

Направление подготовки / специальность: 10.04.01 Информационная безопасность

Направленность (профиль) подготовки: Информационная безопасность автоматизированных систем

Квалификация выпускника: магистр

Форма обучения: очное

Язык обучения: русский

Год начала обучения по образовательной программе: 2023

1. Операционная система Microsoft office professional plus 2010, или Microsoft Windows 7 Профессиональная, или Windows XP (Volume License)
2. Пакет офисного программного обеспечения Microsoft Office 365, или Microsoft office professional plus 2010
3. Adobe Reader XI или Adobe Acrobat Reader DC
4. Браузер Mozilla Firefox
5. Браузер Google Chrome
6. Kaspersky Endpoint Security для Windows
7. Программная система для обнаружения текстовых заимствований в учебных и научных работах. АО «Антиплагиат»
8. Электронная библиотечная система «ZNANIUM.COM»
9. Электронная библиотечная система Издательства «Лань»
10. Электронная библиотечная система «Консультант студента»

Конкретный состав программного обеспечения для практики определяется темой выпускной квалификационной работы. Наиболее часто используются средства из программных систем Visual Studio community edition и IntelliJ IDEA community edition. Рекомендуется для этих целей использовать, в том числе, онлайн компиляторы:

1. <https://www.onlinegdb.com/>
2. <https://cloud.scilab.in/>
3. <https://rextester.com/>

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "ZNANIUM.COM", доступ к которой предоставлен обучающимся. ЭБС "ZNANIUM.COM" содержит произведения крупнейших российских учёных, руководителей государственных органов, преподавателей ведущих вузов страны, высококвалифицированных специалистов в различных сферах бизнеса. Фонд библиотеки сформирован с учетом всех изменений образовательных стандартов и включает учебники, учебные пособия, учебно-методические комплексы, монографии, авторефераты, диссертации, энциклопедии, словари и справочники, законодательно-нормативные документы, специальные периодические издания и издания, выпускаемые издательствами вузов. В настоящее время ЭБС ZNANIUM.COM соответствует всем требованиям федеральных государственных образовательных стандартов высшего образования (ФГОС ВО) нового поколения.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе Издательства "Лань", доступ к которой предоставлен обучающимся. ЭБС Издательства "Лань" включает в себя электронные версии книг издательства "Лань" и других ведущих издательств учебной литературы, а также электронные версии периодических изданий по естественным, техническим и гуманитарным наукам. ЭБС Издательства "Лань" обеспечивает доступ к научной, учебной литературе и научным периодическим изданиям по максимальному количеству профильных направлений с соблюдением всех авторских и смежных прав.

Макет отзыва руководителя выпускной квалификационной работы

ОТЗЫВ

руководителя о выпускной квалификационной работе обучающегося _____ группы
__ курса направления подготовки (специальности) *10.04.01 Информационная безопасность профиля*
Информационная безопасность автоматизированных систем
Институт физики
[Фамилия И.О. обучающегося – автора ВКР в родительном падеже]

[Текст отзыва]

Оценивание параметров текста ВКР

Параметр	Оценка
<i>Актуальность темы и результатов работы</i>	<i>[Отлично, Хорошо, Удовлетворительно, Неудовлетворительно]</i>
<i>Теоретическая и практическая значимость</i>	<i>[Отлично, Хорошо, Удовлетворительно, Неудовлетворительно]</i>
<i>Корректность использованного инструментария</i>	<i>[Отлично, Хорошо, Удовлетворительно, Неудовлетворительно]</i>
<i>Владение профессиональной терминологией</i>	<i>[Отлично, Хорошо, Удовлетворительно, Неудовлетворительно]</i>
<i>Обоснованность выводов</i>	<i>[Отлично, Хорошо, Удовлетворительно, Неудовлетворительно]</i>

*[Ученая степень (при наличии),
ученое звание (при наличии),
должность руководителя ВКР]* _____ *[Фамилия И.О. руководителя ВКР]*
(подпись)

Макет рецензии на выпускную квалификационную работу

РЕЦЕНЗИЯ
на выпускную квалификационную работу обучающегося _____ группы
__ курса направления подготовки (специальности) **10.04.01 Информационная безопасность профиля**
Информационная безопасность автоматизированных систем
Институт физики
[Фамилия И.О. обучающегося – автора ВКР в родительном падеже]

[Текст рецензии]

Оценивание параметров текста ВКР

Параметр	Оценка
<i>Актуальность темы и результатов работы</i>	<i>[Отлично, Хорошо, Удовлетворительно, Неудовлетворительно]</i>
<i>Теоретическая и практическая значимость</i>	<i>[Отлично, Хорошо, Удовлетворительно, Неудовлетворительно]</i>
<i>Корректность использованного инструментария</i>	<i>[Отлично, Хорошо, Удовлетворительно, Неудовлетворительно]</i>
<i>Владение профессиональной терминологией</i>	<i>[Отлично, Хорошо, Удовлетворительно, Неудовлетворительно]</i>
<i>Обоснованность выводов</i>	<i>[Отлично, Хорошо, Удовлетворительно, Неудовлетворительно]</i>

*[Ученая степень (при наличии),
ученое звание (при наличии),
должность рецензента]*

(подпись)

[Фамилия И.О. рецензента]