

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего
образования
«Санкт-Петербургский государственный университет аэрокосмического
приборостроения»

Кафедра № 34 Технологий защиты информации

«УТВЕРЖАЮ»
Проректор по учебно-
воспитательной работе

В.А. Матвеев
(подпись, фамилия)

24 мая 2019 г.

ПРОГРАММА ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

Код направления/специальности	10.05.03
Наименование направления/специальности	Информационная автоматизированных систем
Наименование направления/специальности	Обеспечение безопасности распределенных информационных систем
Форма обучения	очная

Лист согласования
Программы составил(а)

Долгет, К.Э.Н.
Должность, уч. степень, звание


24.05.2019
Подпись, дата

Т.Н. Енина
инициал, фамилия

Программа одобрена на заседании кафедры № 34
«23» мая 2019 г. протокол № 10

Заведующий кафедрой № 34

Д.Н. Дюл.
Должность, уч. степень, звание


24.05.2019
Подпись, дата

С.В. Исидоренко
инициал, фамилия

Ответственный за ОП 10.05.03(07)

Дюл, К.Т.Н., Дюл.
Должность, уч. степень, звание


24.05.2019
Подпись, дата

В.А. Матвеев
инициал, фамилия

Заместитель директора института (декана факультета) № 3 по методической работе

Дюл, К.Т.Н., Дюл.
(Должность, уч. степень, звание)


24.05.2019
Подпись, дата

М.В. Буряков
(инициал, фамилия)

ЦЕЛИ, ЗАДАЧИ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

1.1. Целью ГИА студентов по специальности «10.05.03 «Информационная безопасность автоматизированных систем», направленности «Обеспечение информационной безопасности распределенных информационных систем», видам профессиональной деятельности: научно-исследовательская, проектно-конструкторская, контрольно-аналитическая, организационно-управленческая, эксплуатационная – является установление уровня подготовки студента к выполнению профессиональных задач и соответствия его подготовки, требуемой по ОП квалификации: специалист по защите информации.

1.2. Задачами ГИА являются:

1.2.1. Проверка уровня сформированности компетенций, определенных ФГОС ВО и ОП ГУАП, включающих в себя (компетенции, помеченные «*» выделены для контроля на ГЭ):

*ОК-1 «способность использовать основы философских знаний для формирования мировоззренческой позиции»;

*ОК-2 «способность использовать основы экономических знаний в различных сферах деятельности»;

*ОК-3 «способность анализировать основные этапы и закономерности исторического развития России, её место и роль в современном мире для формирования гражданской позиции и развития патриотизма»;

*ОК-4 «способность использовать основы правовых знаний в различных сферах деятельности»;

*ОК-5 «способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики»;

ОК-6 «способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия»;

*ОК-7 «способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности»;

*ОК-8 «способность к самоорганизации и самообразованию»;

ОК-9 «способность использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности»:

знать – методы и средства физической культуры

уметь - использовать методы и средства физической культуры для обеспечения полноценной правоохранительной деятельности

владеть навыками – физических упражнений;

иметь опыт деятельности – в обеспечении физических тренировок;

*ОПК-1 «способность анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач»;

*ОПК-2 «способность корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники»;

ОПК-3 «способность применять языки, системы и инструментальные средства программирования в профессиональной деятельности»;

*ОПК-4 «способность понимать значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах»;

ОПК-5 «способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами»;

ОПК-6 «способность применять нормативные правовые акты в профессиональной деятельности»;

ОПК-7 «способность применять приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций»;

ОПК-8 «способность к освоению новых образцов программных, технических средств и информационных технологий»;

знать – методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации;

уметь – работать с различными источниками информации, информационными ресурсами и технологиями;

владеть навыками – хранения, поиска, систематизации, обработки и передачи информации;

иметь опыт деятельности – по использованию информационных ресурсов для обработки информации;

*ПК-1 «способность осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке»;

- ПК-2 «способность создавать и исследовать модели автоматизированных систем»;
- ПК-3 «способность проводить анализ защищенности автоматизированных систем»;
- ПК-4 «способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы»;
- ПК-5 «способность проводить анализ рисков информационной безопасности автоматизированной системы»;
- ПК-6 «способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности»;
- ПК-7 «способность разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ»;
- ПК-8 «способность разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем»;
- ПК-9 «способность участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности»;
- ПК-10 «способность применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности»;
- ПК-11 «способность разрабатывать политику информационной безопасности автоматизированной системы»;
- ПК-12 «способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы»;
- ПК-13 «способность участвовать в проектировании средств защиты информации автоматизированной системы»;
- ПК-14 «способность проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации»;
- ПК-15 «способность участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты автоматизированных систем»;
- ПК-16 «способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации»;
- ПК-17 «способность проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации»;

ПК-18 «способность организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности»;

ПК-19 «способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы»;

ПК-20 «способность организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности»;

ПК-21 «способность разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем»;

ПК-22 «способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации»;

ПК-23 «способность формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа»;

ПК-24 «способность обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности»;

ПК-25 «способность обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении не штатных ситуаций»;

ПК-26 «способность администрировать подсистему информационной безопасности автоматизированной системы»;

ПК-27 «способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы»;

ПК-28 «способность управлять информационной безопасностью автоматизированной системы»;

знать – состав модулей в области информационных технологий и информационной безопасности;

уметь – определять уровень освоения дисциплин;

владеть навыками – оценки результаты образовательного процесса;

иметь опыт деятельности – по контролю результатов образовательного процесса в области информационных технологий и информационной безопасности;

ПСК-7.1 «способность разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах»;

ПСК-7.2 «способность проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах»;

ПСК-7.3 «способность проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем»;

ПСК-7.4 «способность проводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах»;

ПСК-7.5 «способность координировать деятельность подразделений и специалистов по защите информации на предприятии, в учреждении, организации»:

знать – правила и этапы проектирования информационных систем;

уметь – проектировать структуру и состав информационной системы;

владеть навыками – выбора способа реализации информационной системы;

иметь опыт деятельности – по выбору программно-аппаратного обеспечения информационной системы.

1.2.2. Принятие решения о присвоении квалификации по результатам ГИА и выдаче документа о высшем образовании и присвоении квалификации.

2 ФОРМЫ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

В Блок «Государственная итоговая аттестация» входит защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты, а также подготовка к сдаче и сдача государственного экзамена.

ГИА проводится в форме:

- государственный экзамен (ГЭ) «Подготовка к сдаче и сдача государственного экзамена»;
- защита выпускной квалификационной работы (ВКР).

3 ОБЪЕМ И ПРОДОЛЖИТЕЛЬНОСТЬ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

Объем и продолжительность ГИА указаны в таблице 1.

Таблица 1 – Объем и продолжительность ГИА

№ семестра	Трудоемкость ГИА (ЗЕ)	Продолжительность в неделях
10	9	6

4 ПРОГРАММА ГОСУДАРСТВЕННОГО ЭКЗАМЕНА

4.1. Программа государственного экзамена.

4.1.1. Форма проведения ГЭ – письменная.

4.1.2. Перечень компетенций, освоение которых оценивается на ГЭ, приведен в таблице

2.

Таблица 2 – Перечень компетенций, уровень освоения которых оценивается на ГЭ

ОК-1 «способность использовать основы философских знаний для формирования мировоззренческой позиции»
Культурология
Философия
Психология и педагогика
Социальная психология
Социология и политология
ОК-2 «способность использовать основы экономических знаний в различных сферах деятельности»
Экономика
Международный бизнес
Мировая экономика
Защита банковской информации
Прикладная экономика

Технологии защиты электронных платежей
Основы управленческой деятельности
Экономика проектов в информационных технологиях
ОК-3 «способность анализировать основные этапы и закономерности исторического развития России, её место и роль в современном мире для формирования гражданской позиции и развития патриотизма»
История
Правоведение
ОК-4 «способность использовать основы правовых знаний в различных сферах деятельности»
Социология и политология
Правоведение
ОК-5 «способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики»
Введение в специальность
Информационные технологии
Теория информации
Стандарты информационной безопасности
Основы управленческой деятельности
Управление информационной безопасностью
Организационное и правовое обеспечение информационной безопасности
Информационная безопасность распределенных информационных систем
ОК-6 «способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия»
История
Философия
Социальная психология
Психология и педагогика
Защита информации в распределенных информационных системах
Проектирование безопасных информационных систем
Основы управленческой деятельности
Управление информационной безопасностью
Научно-технический семинар
Научно-исследовательская работа
ОК-7 «способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности»
Экология
Экономика
Иностранный язык
Введение в специальность
Промышленная экология

Культурология
Социальная психология
Психология и педагогика
Правоведение
Криптографические методы защиты информации
Мировая экономика
Международный бизнес
Научно-технический семинар
Экономика проектов в информационных технологиях
Научно-исследовательская работа
Прикладная экономика
ОК-8 «способность к самоорганизации и самообразованию»
История
Алгебра и геометрия
Математическая логика и теория алгоритмов
Информатика
Математический анализ
Иностранный язык
Экономика
Дискретная математика
Физика
Культурология
Философия
Информационные технологии
Теория вероятностей и математическая статистика
Социология и политология
Электротехника
Основы радиотехники
Вычислительная математика
Математические основы обработки информации
Теория информации
Международный бизнес
Мировая экономика
Теория кодирования
Исследование операций и теории игр
Прикладная экономика
Экономика проектов в информационных технологиях
ОК-9 «способность использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности»
Физическая культура (элективный модуль)
Безопасность жизнедеятельности
Физическая культура
ОПК-1 «способность анализировать физические

явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач»
Математический анализ
Математическая логика и теория алгоритмов
Физика
Теория вероятностей и математическая статистика
Электротехника
Инженерная графика
Основы радиотехники
Вычислительная математика
Технологии и методы программирования
Электроника и схемотехника
Мультимедиа технологии
Технологии обработки аудио- и видеоданных
Устройства и системы беспроводной связи
Организация ЭВМ и вычислительных систем
Метрология
Микропроцессорная техника
Математические основы обработки информации
Моделирование систем
Системное программное обеспечение
Операционные системы
Распределенные информационные системы
Постквантовая криптография
Безопасность сетей ЭВМ
Распределенные сети хранения данных
Безопасность операционных систем
Языки программирования
Теория графов и ее приложения
Исследование операций и теории игр
Научно-исследовательская работа
Защита информации в сенсорных сетях
ОПК-2 «способность корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники»
Математическая логика и теория алгоритмов
Алгебра и геометрия
Математический анализ
Дискретная математика
Физика

Инженерная графика
Теория вероятностей и математическая статистика
Вычислительная математика
Математические основы обработки информации
Теория кодирования
Постквантовая криптография
Исследование операций и теории игр
Теория графов и ее приложения
ОПК-3 «способность применять языки, системы и инструментальные средства программирования в профессиональной деятельности»
Информатика
Основы программирования
Технологии и методы программирования
Криптографические методы защиты информации
Программно-аппаратные средства обеспечения информационной безопасности
Методы и средства проектирования информационных систем
Языки программирования
Научно-исследовательская работа
ОПК-4 «способность понимать значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах»
Промышленная экология
Информатика
Экология
Основы программирования
Информационные технологии
Основы информационной безопасности
Технологии и методы программирования
Безопасность жизнедеятельности
Теория информации
Теория информационной безопасности
Моделирование систем
Техническая защита информации
Языки программирования
Защита информации в распределенных информационных системах
Научно-исследовательская работа
Информационная безопасность распределенных информационных систем
Технология построения защищенных распределенных приложений
ОПК-5 «способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами»
Инженерная графика
Криптографические методы защиты информации
Научно-исследовательская работа

Научно-технический семинар
ОПК-6 «способность применять нормативные правовые акты в профессиональной деятельности»
Стандарты информационной безопасности
Метрология
Микропроцессорная техника
Теория информационной безопасности
Организационное и правовое обеспечение информационной безопасности
ОПК-7 «способность применять приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций»
Промышленная экология
Экология
Безопасность жизнедеятельности
ОПК-8 «способность к освоению новых образцов программных, технических средств и информационных технологий»
Основы радиотехники
Архитектура информационных систем
Электроника и схемотехника
Организация ЭВМ и вычислительных систем
Программно-аппаратные средства обеспечения информационной безопасности
Сети и системы передачи информации
Моделирование систем
Теория кодирования
Безопасность систем баз данных
Методы и средства проектирования информационных систем
Разработка и эксплуатация защищенных автоматизированных систем
Надежность информационных систем
Проектирование безопасных информационных систем
Разработка мобильных приложений
Технология построения защищенных распределенных приложений
ПК-1 «способность осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке»
Основы программирования
Теория графов и ее приложения
Научно-технический семинар
ПК-2 «способность создавать и исследовать модели автоматизированных систем»
Устройства и системы беспроводной связи
Методы проектирования защищенных распределенных информационных систем
ПК-3 «способность проводить анализ защищенности автоматизированных систем»
Распределенные сети хранения данных
Распределенные информационные системы
Информационная безопасность распределенных информационных систем

Методы проектирования защищенных распределенных информационных систем
ПК-4 «способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы»
Технологии защиты от скрытой передачи данных
Защита от вредоносных программ
Технологии защиты электронных платежей
Защита банковской информации
Научно-исследовательская работа
ПК-5 «способность проводить анализ рисков информационной безопасности автоматизированной системы»
Системное программное обеспечение
Операционные системы
Информационная безопасность распределенных информационных систем
ПК-6 «способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности»
Основы информационной безопасности
Безопасность сетей ЭВМ
Безопасность систем баз данных
Техническая защита информации
Безопасность операционных систем
Разработка мобильных приложений
ПК-7 «способность разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ»
Стандарты информационной безопасности
Базы данных
Сети и системы передачи информации
Методы и средства проектирования информационных систем
Разработка и эксплуатация защищенных автоматизированных систем
Проектирование безопасных информационных систем
ПК-8 «способность разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем»
Базы данных
Интеллектуальные системы и технологии
Методы проектирования защищенных распределенных информационных систем
Технология построения защищенных распределенных приложений
ПК-9 «способность участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности»
Постквантовая криптография
Техническая защита информации
Разработка мобильных приложений
Технология построения защищенных распределенных приложений
ПК-10 «способность применять знания в области электроники и схемотехники,

технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности»
Электротехника
Электроника и схемотехника
Основы радиотехники
Метрология
Микропроцессорная техника
Сети и системы передачи информации
Научно-исследовательская работа
ПК-11 «способность разрабатывать политику информационной безопасности автоматизированной системы»
Основы информационной безопасности
Стандарты информационной безопасности
Безопасность операционных систем
Безопасность систем баз данных
Безопасность сетей ЭВМ
Защита информации в сенсорных сетях
ПК-12 «способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы»
Мультимедиа технологии
Технологии обработки аудио- и видеоданных
Защита информации в распределенных информационных системах
ПК-13 «способность участвовать в проектировании средств защиты информации автоматизированной системы»
Распределенные сети хранения данных
Распределенные информационные системы
Защита от вредоносных программ
Защита информации в распределенных информационных системах
Защита информации в сенсорных сетях
Технологии защиты электронных платежей
Защита банковской информации
Разработка мобильных приложений
ПК-14 «способность проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации»
Архитектура информационных систем
Системное программное обеспечение
Операционные системы
Методы и средства проектирования информационных систем
Надежность информационных систем
ПК-15 «способность участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты автоматизированных систем»

Научно-исследовательская работа
Защита информации в сенсорных сетях
ПК-16 «способность участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации»
Интеллектуальные системы и технологии
Организационное и правовое обеспечение информационной безопасности
ПК-17 «способность проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации»
Программно-аппаратные средства обеспечения информационной безопасности
Разработка и эксплуатация защищенных автоматизированных систем
Защита от вредоносных программ
Проектирование безопасных информационных систем
ПК-18 «способность организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности»
Введение в специальность
Проектирование безопасных информационных систем
ПК-19 «способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы»
Устройства и системы беспроводной связи
Технологии обработки аудио- и видеоданных
Мультимедиа технологии
Научно-исследовательская работа
Технологии защиты электронных платежей
Защита банковской информации
ПК-20 «способность организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности»
Технологии защиты от скрытой передачи данных
Проектирование безопасных информационных систем
ПК-21 «способность разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем»
Технологии защиты от скрытой передачи данных
Организационное и правовое обеспечение информационной безопасности
ПК-22 «способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации»
Методы и средства проектирования информационных систем
Разработка мобильных приложений
ПК-23 «способность формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа»
Разработка и эксплуатация защищенных автоматизированных систем

Защита информации в сенсорных сетях
ПК-24 «способность обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности»
Устройства и системы беспроводной связи
Разработка мобильных приложений
Научно-технический семинар
Защита информации в сенсорных сетях
ПК-25 «способность обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении не штатных ситуаций»
Распределенные сети хранения данных
Распределенные информационные системы
Защита банковской информации
Технологии защиты электронных платежей
ПК-26 «способность администрировать подсистему информационной безопасности автоматизированной системы»
Распределенные сети хранения данных
Распределенные информационные системы
Информационная безопасность распределенных информационных систем
ПК-27 «способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы»
Системное программное обеспечение
Операционные системы
Методы проектирования защищенных распределенных информационных систем
ПК-28 «способность управлять информационной безопасностью автоматизированной системы»
Распределенные сети хранения данных
Распределенные информационные системы
Защита информации в распределенных информационных системах
Технология построения защищенных распределенных приложений
ПСК-7.1 «способность разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах»
Защита информации в распределенных информационных системах
Методы проектирования защищенных распределенных информационных систем
ПСК-7.2 «способность проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах»
Методы проектирования защищенных распределенных информационных систем
ПСК-7.3 «способность проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем»
Исследование операций и теории игр

Технология построения защищенных распределенных приложений
ПСК-7.4 «способность проводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах»
Теория графов и ее приложения
Информационная безопасность распределенных информационных систем
ПСК-7.5 «способность координировать деятельность подразделений и специалистов по защите информации на предприятии, в учреждении, организации»
Информационная безопасность распределенных информационных систем

4.1.3. Методические рекомендации обучающимся по подготовке к ГЭ.

Государственный экзамен (ГЭ) – является составной частью Государственной итоговой аттестации (ГИА) и представляет собой форму оценки знаний, навыков самостоятельной работы, и способности применять их для решения практических задач, полученных обучающимся в процессе освоения образовательной программы (ОП) за весь период обучения. К ГИА допускается студент, не имеющий академической задолженности и в полном объеме выполнивший учебный план или индивидуальный учебный план по соответствующей ОП ВО.

ГЭ проводится по нескольким дисциплинам ОП, результаты освоения которых имеют определяющее значение для профессиональной деятельности выпускников. ГЭ проводится в письменной форме в период после завершения преддипломной практики и завершается аттестационной оценкой «отлично», «хорошо», «удовлетворительно», «неудовлетворительно», оформляемой протоколом Государственной экзаменационной комиссии (ГЭК).

Вопросы, выносимые на ГЭ, список рекомендуемой литературы для подготовки к ГЭ, критерии оценки результатов сдачи государственных экзаменов, а также порядок проведения ГЭ, порядок подачи и рассмотрения апелляций, доводятся до сведения студентов не позднее, чем за шесть месяцев до даты проведения ГЭ.

В период подготовки к ГЭ обучающемуся рекомендуется подготовить обстоятельные ответы на все вопросы, выносимые на ГЭ, используя рекомендуемую для подготовки к ГЭ литературу, а также посетить консультации, проводимые перед ГЭ. Ответы обучающегося должны продемонстрировать глубокое и всестороннее усвоение учебного материала образовательной программы (ОП), уверенное, логичное, последовательное и грамотное его изложение, знание основной и дополнительной литературы с тесной привязкой усвоенных научных положений к практической деятельности, умелое обоснование и аргументацию идей, выдвигаемых обучающимся в

тексте ответа, с соответствующими выводами и обобщениями, свободное владение системой специализированных понятий.

4.1.4. Перечень рекомендуемой литературы, необходимой при подготовке к ГЭ, приводится в разделе 7 программы ГИА.

4.1.5. Перечень вопросов для ГЭ приводится в таблицах 9–11 раздела 10 программы ГИА.

4.1.6. Методические указания по процедуре проведения ГЭ по направлению, определяемые выпускающей кафедрой

ГИА проводится в сроки, предусмотренные учебным планом образовательной программы и графиком учебного процесса.

Перед государственными экзаменами проводится консультирование студентов по вопросам, включенным в программу государственного экзамена (далее – предэкзаменационные консультации).

Студенты обеспечиваются программами государственных экзаменов, включающими в себя перечень вопросов, выносимых на государственный экзамен, и рекомендации по подготовке к государственному экзамену, в том числе перечень рекомендуемых источников для подготовки к государственному экзамену.

Члены сформированной приказом Ректора ГУАП ГЭК по кафедре № 34 готовят экзаменационные билеты для проведения ГЭ согласно списку вопросов для ГЭ, приведенных в таблицах 9–11 раздела 10 программы ГИА (каждый билет включает пять вопросов). Секретарь ГЭК оформляет экзаменационные билеты согласно нормативным документам ГУАП; в установленные сроки доводит до сведения обучающихся вопросы, выносимые на ГЭ, список рекомендуемой литературы для подготовки к ГЭ, график проведения заседаний ГЭК по приему ГЭ (дата, время и место проведения ГЭ), график проведения консультаций обучающихся по подготовке к ГЭ и список обучающихся, допущенных к ГИА. Перед проведением заседания ГЭК по приему ГЭ готовит список обучающихся, допущенных к ГЭ и соответствующие бланки протоколов заседания ГЭК.

Во время проведения государственного экзамена в письменной форме в аудитории должно находиться не менее двух членов ГЭК. Возможно установление графика пребывания членов ГЭК в аудитории. Проверка письменной работы каждого студента, сдающего государственный экзамен, осуществляется в составе не менее двух третей от состава ГЭК.

Заседания ГЭК проводятся председателем ГЭК.

Решения ГЭК принимаются на закрытых заседаниях с участием не менее двух третей состава, простым большинством голосов членов ГЭК, участвующих в заседании, при обязательном присутствии председателя. При равном числе голосов председатель ГЭК.

Результаты любого из видов государственных аттестационных испытаний, включённых в состав ГИА, определяются оценками по пятибалльной системе оценивания: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Оценки «отлично», «хорошо», «удовлетворительно» означают успешное прохождение государственного аттестационного испытания.

Решения, принятые ГЭК, оформляются протоколами заседаний.

В протоколе заседания локальной ГЭК отражаются перечень заданных студенту вопросов и характеристика ответов на них, мнения членов локальной ГЭК о выявленном в ходе государственного аттестационного испытания уровне подготовленности студента к решению профессиональных задач, а также о выявленных недостатках в теоретической и практической подготовке студента.

Протоколы заседаний ГЭК подписываются председателем и секретарем ГЭК. Секретарь ГЭК в протоколе отмечает, кто из членов ГЭК присутствовал на заседании.

Результаты государственных аттестационных испытаний, проводимых в письменной форме, объявляются секретарем ГЭК студентам не позднее следующего рабочего дня после проведения государственного аттестационного испытания. Для объявления результатов студентам могут быть использованы: корпоративная электронная почта студентов.

Студент, пропустивший государственный экзамен по неуважительной причине, либо получивший неудовлетворительную оценку, не допускается к следующему государственному аттестационному испытанию и отчисляется как не выполнивший обязанностей по добросовестному освоению образовательной программы и выполнению учебного плана.

К защите ВКР допускаются студенты, успешно сдавшие все государственные экзамены и представившие ВКР в установленный срок. Лица, нарушившие установленный срок, и не допущенные к защите ВКР, в том числе по причине нарушений, выявленных в ходе обязательной проверки текста ВКР на плагиат, отчисляются как не выполнившие обязанностей по добросовестному освоению образовательной программы и выполнению учебного плана.

Во время проведения ГИА студентам запрещается иметь при себе и использовать любые средства передачи информации (электронные средства связи).

Обнаружение у студентов во время государственного аттестационного испытания несанкционированных учебных и методических материалов, электронных средств связи является основанием для принятия решения о выставлении оценки «неудовлетворительно», вне зависимости от того, были ли использованы указанные материалы (средства) при подготовке ответа.

В период подготовки к государственному экзамену студентам должны быть предоставлены необходимые предэкзаменационные консультации по дисциплинам, вошедшим в программу государственного экзамена.

Государственный экзамен проводится письменно.

При проведении государственного экзамена студенты получают экзаменационные билеты, содержащие задания, составленные в соответствии с утверждённой программой проведения государственного экзамена.

При проведении государственного экзамена в письменной форме на экзамен выделяется до четырех академических часов. Оценки формируются на основе результатов выполнения экзаменационных заданий по методике, утвержденной в программе проведения государственного экзамена.

По завершении государственного экзамена ГЭК на закрытом заседании обсуждает ответы каждого студента или его письменную работу (после соответствующей проверки) и выставляет каждому студенту согласованную итоговую оценку в соответствии с утвержденными критериями оценивания.

В случае расхождения мнения членов ГЭК по итоговой оценке на основе оценок, поставленных каждым членом ГЭК в отдельности, решение ГЭК принимается простым большинством голосов членов ГЭК, участвующих в заседании, при обязательном присутствии председателя ГЭК. При равном числе голосов председатель обладает правом решающего голоса.

Итоговая оценка за экзамен по пятибалльной системе оценивания проставляется в протокол заседания ГЭК. В протоколе заседания фиксируются также задания, по которым проводился государственный экзамен.

Письменные экзаменационные работы формируются в отдельное дело и в обязательном порядке хранятся до окончания календарного года и могут быть запрошены АК при рассмотрении заявления студента об апелляции результатов ГИА.

5 ТРЕБОВАНИЯ К ВЫПУСКНЫМ КВАЛИФИКАЦИОННЫМ РАБОТАМ И ПОРЯДКУ ИХ ВЫПОЛНЕНИЯ

5.1. Состав и содержание разделов (глав) ВКР, определяемые спецификой ОП.

Тема и содержание ВКР должны соответствовать специальности, требованиям ФГОС ВО и работодателей, а также отвечать современным тенденциям развития науки и техники.

Согласно требованиям ФГОС ВО, учебных планов и программ ГИА по специальностям 10.05.03 и 10.05.05, дипломные работы студентов должны отражать один или несколько видов профессиональной деятельности выпускников:

Укрупненная группа подготовки: 10.00.00 Информационная безопасность. Уровень высшего образования: специалитет. Специальность: 10.05.03 Информационная безопасность автоматизированных систем. Специализация: 10.05.03.07 Обеспечение информационной безопасности распределенных информационных систем. Виды профессиональной деятельности выпускников:

- научно-исследовательская;
 - сбор, обработка, анализ и систематизация научно-технической информации по проблематике информационной безопасности автоматизированных систем;
 - подготовка научно-технических отчетов, обзоров, докладов, публикаций по результатам выполненных исследований;
 - моделирование и исследование свойств защищенных автоматизированных систем;
 - анализ защищенности информации в автоматизированных системах и безопасности реализуемых информационных технологий;
 - разработка эффективных решений по обеспечению информационной безопасности автоматизированных систем.
- проектно-конструкторская;
 - сбор и анализ исходных данных для проектирования защищенных автоматизированных систем;
 - разработка политик информационной безопасности автоматизированных систем;
 - разработка защищенных автоматизированных систем в сфере профессиональной деятельности, обоснование выбора способов и средств защиты информационно-технологических ресурсов автоматизированных систем;
 - выполнение проектов по созданию программ, комплексов программ, программно-аппаратных средств, баз данных, компьютерных сетей для защищенных автоматизированных систем;
 - разработка систем управления информационной безопасностью автоматизированных систем.
- контрольно-аналитическая;

- контроль работоспособности и эффективности применяемых средств защиты информации;
- выполнение экспериментально-исследовательских работ при сертификации средств защиты информации и аттестации автоматизированных систем;
- проведение инструментального мониторинга защищенности автоматизированных систем и анализа его результатов.
 - организационно-управленческая;
- организация работы коллектива, принятие управленческих решений в условиях спектра мнений, определение порядка выполнения работ;
- организационно-методическое обеспечение информационной безопасности автоматизированных систем;
- организация работ по созданию, внедрению, эксплуатации и сопровождению защищенных автоматизированных систем;
- контроль реализации политики информационной безопасности.
 - эксплуатационная
- реализация информационных технологий в сфере профессиональной деятельности с использованием защищенных автоматизированных систем;
- администрирование подсистем информационной безопасности автоматизированных систем;
- мониторинг информационной безопасности автоматизированных систем;
- управление информационной безопасностью автоматизированных систем;
- обеспечение восстановления работоспособности систем защиты информации при возникновении нештатных ситуаций.

Объем текста дипломной работы специалиста (без учета списка использованных источников и приложений) должен составлять от 60 до 100 листов формата А4. Текст должен быть изложен грамотно, без орфографических и стилистических ошибок, с правильным использованием терминологического научного аппарата и специальной терминологии. Несоответствие ВКР данному требованию отмечается в отзыве руководителя ВКР о работе студента в период подготовки ВКР (далее – отзыв).

Тема ВКР может иметь либо практическую, либо научную направленность, что определяет структуру ВКР и ее содержание.

Текст ВКР должен включать в себя следующие структурные элементы, формы которых утверждены РДО ГУАП. СМК 3.160:

- 1) Титульный лист
- 2) Задание на ВКР

- 3) Реферат (аннотация)
- 4) Содержание
- 5) Определения, обозначения, сокращения, нормативные ссылки
- 6) Введение
- 7) Основная часть
- 8) Заключение
- 9) Список использованных источников
- 10) Приложения (при наличии)

5.2. Дополнительные компоненты ВКР, определяемые выпускающей кафедрой.

Программный код разработанного приложения приводится в приложении к пояснительной записке.

5.3. Наличие/отсутствие реферата в структуре ВКР.

Реферат ВКР оформляется на отдельной странице и должен кратко передавать основное содержание работы, объем реферата не должен превышать 3 страниц. Реферат должен содержать перечень ключевых слов (от 5 до 10), характеризующих содержание ВКР и обеспечивающих возможность информационного поиска.

Пример:

Ключевые слова: информационная система, защита информации, нейронные сети, инциденты информационной безопасности, бизнес-процессы.

В тексте реферата должны быть указаны следующие элементы:

- актуальность темы исследования;
- цель и задачи работы;
- предмет и объект исследования;
- область применения;
- методы и средства разработки;
- основные результаты работы;
- практическая значимость результатов (при наличии);
- экономическая эффективность (при наличии).

5.4. Требования к структуре иллюстративно–графического материала (презентация, плакаты, чертежи).

Выступление студента на защите ВКР может сопровождаться показом иллюстративно-графического материала – плакатов или презентаций с использованием мультимедийной техники.

Для защиты дипломной работы по специальности 10.05.03 рекомендуется следующая структура иллюстративно-графического материала:

1. На первом слайде следует указать название вуза, название кафедры, название вида ВКР (дипломная работа), тема работы, ФИО автора, номер группы, ФИО научного руководителя, город и год.

2. Далее рекомендуется разместить материал, подтверждающий актуальность разрабатываемой темы, описание объекта и предмета исследования, современное состояние дел в данной предметной области.

3. Слайд, содержащий цель и задачи работы.

4. Далее на слайдах следует представить информацию о современных достижениях науки и технологиях, касающихся решения рассматриваемой проблемы (патентный поиск). Необходимо указать достоинства и недостатки обнаруженных решений.

5. Описание методов исследования, средств и технологий, используемых в работе.

6. Группа слайдов, отражающих основные этапы работы и достигнутые в их ходе результаты.

7. В заключительной части следует подвести итог выполненной работы: практическая или научная значимость полученных результатов и собственный вклад студента.

Рекомендуется использовать 10-20 слайдов, так как меньшее количество не позволит всесторонне оценить представленную работу, а большее количество приведет к нарушению норм времени, отводимого на защиту.

Слайды в обязательном порядке должны быть пронумерованы.

Существуют следующие рекомендации по оформлению слайдов:

- все слайды должны быть выдержаны в едином стиле, рекомендуется использовать один-два оттенка цвета, один тип шрифта, а также одинаковый размер шрифта для заголовков и один размер для основного текста.
- используемые цветовые гаммы должны быть максимально контрастными – черный шрифт на белом фоне или белый шрифт на черном фоне. Размер шрифта должен быть достаточен для «читаемости» слайда (как правило, не менее 18 пт.).
- рекомендуется свести к минимуму эффекты анимации, так как они значительно усложняют и удлиняют процесс защиты.

- крайне нежелательно дублировать на слайдах текст, произносимый студентами в докладе (кроме цели и задач работы и заключения). Информация на слайдах должна дополнять доклад, в основном с помощью графического, иллюстративного материала, а также формул и таблиц. Большие блоки текста на слайдах бесполезны.
- нумерация рисунков, диаграмм, таблиц и схем может проводиться независимо от их номеров в тексте ВКР, начиная с номера 1.
- при представлении больших таблиц на слайдах необходимо проанализировать возможность их разделения на несколько мелких.

5.5. Требования к защите ВКР, определяемые выпускающей кафедрой в соответствии с локальными нормативными актами ГУАП.

Законченная ВКР, подписанная студентом, представляется руководителю, который составляет на нее отзыв. Отзыв руководителя ВКР должен содержать оценку:

- актуальности темы;
- полноты решения поставленных задач;
- степени самостоятельности и инициативности студента;
- умения студента пользоваться специальной литературой;
- способности студента к исследовательской работе;
- возможности использования полученных результатов на практике;
- возможности присвоения выпускнику соответствующей квалификации.

Решение о допуске к защите принимает рабочая комиссия, которая заслушивает сообщение студента по ВКР, определяет ее соответствие выданному заданию, выясняет степень готовности студента к защите, знакомится с отзывом руководителя.

Затем ВКР, отзыв руководителя, решение рабочей комиссии предоставляются заведующему кафедрой, который дает заключение о возможности допуска студента к защите. Допуск студента к защите фиксируется подписью заведующего кафедрой на титульном листе пояснительной записки к ВКР и иллюстративных (графических) материалах.

ВКР, допущенная выпускающей кафедрой к защите, заведующим кафедрой направляется на рецензию. Рецензентами дипломных работ выступают лица из числа профессорско-преподавательского состава других кафедр ГУАП, главных и ведущих специалистов по профилю работы, занятых в организациях соответствующей отрасли, научных учреждениях, педагогического состава других вузов. В рецензии должны быть отмечены:

- актуальность темы работы;

- степень соответствия работы заданию;
- соответствие содержания пояснительной записки требованиям стандарта;
- наличие критического обзора литературы, его полнота и последовательность анализа;
- полнота описания методики расчетов или проведенных исследований и оценка достоверности полученных результатов;
- наличие аргументированных выводов по результатам работы;
- практическая значимость работы;
- недостатки и слабые стороны работы;
- замечания по оформлению пояснительной записки к дипломной работе и стилю изложения материала;

Завершающим этапом выполнения работы является ее защита перед Государственной экзаменационной комиссией (ГЭК).

Защита ВКР проводится путем устного доклада выпускника по иллюстративным (графическим) материалам, которые разрешается представлять с помощью мультимедийных средств (в виде презентации). На доклад студенту отводится до 10 минут. В своем выступлении студент должен кратко обосновать выбор темы исследования, ее актуальность и практическую значимость, представить основное содержание работы. Особое внимание в докладе необходимо уделить выводам и предложениям, сформулированным по результатам выполнения работы.

После доклада выпускник отвечает на вопросы членов ГЭК. Вопросы могут касаться как темы выполненной работы, так и носить общий характер в пределах дисциплин специальности и специализации, изучаемых на протяжении срока обучения в вузе. После членов ГЭК с разрешения председателя вопросы могут задавать все присутствующие на защите.

После ответов выпускника на все заданные ему вопросы выступает рецензент или зачитывается его рецензия. При имеющихся замечаниях рецензента выпускник должен ответить на них. В заключение выступает со своим отзывом руководитель ВКР или при его отсутствии зачитывается отзыв. Защита заканчивается предоставлением выпускнику заключительного слова, в котором он вправе высказать свое мнение по замечаниям и рекомендациям, сделанным в процессе защиты ВКР.

После публичной защиты ВКР проводится закрытое совещание членов ГЭК, на котором обсуждаются результаты защиты, и определяется общая оценка подготовки и защиты ВКР каждого студента. Результаты защиты объявляются председателем ГЭК в день защиты после закрытого заседания комиссии и оформления соответствующих

протоколов. Вместе с объявлением оценок председатель ГЭК зачитывает решение комиссии о присвоении студентам-выпускникам соответствующей квалификации.

Критерии оценки.

Оценка «отлично» выставляется при условии выполнения следующих требований:

- представленная дипломная работа соответствует всем установленным критериям;
- тематика дипломной работы соответствует содержанию одного или нескольких профессиональных модулей;
- содержание дипломной работы соответствует заявленной теме, тема раскрыта полностью;
- обзор литературы и источников отличается полнотой и обстоятельностью, соответствует выбранной теме;
- экспериментальная часть характеризуется актуальностью, оригинальностью, новизной, ценностью поставленных задач, поставленные задачи сформулированы четко и ясно и соответствуют теме, исследование по поставленным задачам проведено в полном объеме, материал экспериментальной части приведен в наглядной форме, продемонстрирован достаточный уровень практических умений и результатов приобретенного практического опыта;
- оформление соответствует установленным нормам и требованиям;
- доклад студента по всем показателям демонстрирует в полном объеме овладение общими и профессиональными компетенциями, предусмотренными ФГОС, учебными программами дисциплин и профессиональных модулей;
- студент ориентируется во всех дополнительных вопросах.

Оценка «хорошо» выставляется при условии выполнения следующих требований:

- тематика дипломной работы соответствует содержанию одного или нескольких профессиональных модулей;
- представленная дипломная работа соответствует всем или почти всем установленным критериям на хорошем уровне (не допускается несоответствие содержания заявленной тематике и требованиям по оформлению);
- доклад студента показывает хорошее усвоение теоретического материала, овладение общими и профессиональными компетенциями, предусмотренными ФГОС, учебными программами дисциплин и профессиональных модулей;
- студент готов к конкретным видам профессиональной деятельности техника по защите информации;
- студент ориентируется во всех дополнительных вопросах, при этом возможны некоторые неточности.

Оценка «удовлетворительно» выставляется в случае, если выполняются следующие условия:

- тематика дипломной работы соответствует содержанию одного или нескольких профессиональных модулей;
- представленная дипломная работа удовлетворяет всем требованиям по оформлению, соответствует заявленной теме, однако имеются существенные недостатки по её содержанию;
- студент показывает неполное усвоение теоретического материала, овладение общими и профессиональными компетенциями, предусмотренными ФГОС, учебными программами дисциплин и профессиональных модулей, отвечает не на все дополнительные вопросы;
- приложения удовлетворительного качества или не представлены.

Оценка «неудовлетворительно» выставляется в случае полного несоответствия дипломной работы установленным требованиям, в процессе защиты студент не владеет теоретическим и практически материалом, наглядный материал не представлен.

5.6. Методические указания по процедуре выполнения ВКР по направлению, определяемые выпускающей кафедрой в соответствии с локальными нормативными актами ГУАП

Подготовка ВКР начинается с выбора темы. Темы предлагаемых студентам дипломных работ, утвержденные приказом ГУАП, доводятся до сведения студентов не позднее, чем за 6 месяцев до начала ГИА.

Студент может выбрать тему ВКР из утвержденного перечня или предложить свою тему, обосновав целесообразность ее разработки и получив согласие заведующего кафедрой. В обоих случаях выбор должен быть подтвержден заявлением студента на имя заведующего выпускающей кафедры по форме, утвержденной РДО ГУАП. СМК 3.160.

Распределение тем ВКР и закрепление руководителей и рецензентов утверждается приказом ГУАП не позднее, чем за два месяца до даты начала защит.

В течение недели с момента утверждения темы ВКР студент получает от руководителя задание на выполнение ВКР по форме, утвержденной РДО ГУАП. СМК 3.160.

После получения задания на ВКР студент осуществляет самостоятельную разработку ВКР. При этом руководитель ВКР оказывает студенту помощь в организации работы, проводит для студентов систематические консультации, проверяет выполнение работы (отдельно по частям или в целом). Форма взаимодействия студента с

руководителем и график выполнения ВКР определяется руководителем по согласованию со студентом.

Завершенная ВКР представляется студентом заведующему кафедрой, который назначает (при необходимости) предварительное рассмотрение (предзащиту) ВКР на выпускающей кафедре. По результатам предзащиты студент может осуществить доработку ВКР с учетом полученных замечаний и рекомендаций.

После доработки ВКР студент представляет ее текст ответственному лицу на выпускающей кафедре для проверки его на объем заимствования, в том числе содержательного с учетом требований настоящих рекомендаций в срок не позднее 20 календарных дней до предполагаемой даты защиты. Результаты проверки будут отражены в отзыве руководителя ВКР.

Завершенная и переплетенная ВКР представляется студентом руководителю ВКР на рассмотрение в срок не позднее 15 календарных дней до предполагаемой даты защиты, которая определяется на основании расписания государственных аттестационных испытаний. Не позднее 10 календарных дней до предполагаемой даты защиты, руководитель подготавливает отзыв, а также ставит подпись на титульном листе ВКР. При выявленном недопустимым объеме неправомерных заимствований, руководитель отметит этот факт в отрицательном отзыве. *После получения отзыва руководителя вносить изменения в текст ВКР недопустимо!*

Студент, получивший отрицательный отзыв руководителя к защите не допускается и отчисляется из ГУАП, как не выполнивший обязанности по освоению образовательной программы и выполнению учебного плана.

После получения отзыва руководителя необходимо пройти проверку работы заведующим выпускающей кафедрой на соответствие нормативным требованиям. При наличии задания, положительного отзыва, необходимых подписей руководителя и студента, результатов проверки на объем заимствований, заведующий кафедрой подписывает титульный лист ВКР.

Подписанная заведующим кафедрой ВКР направляется рецензенту, утвержденному приказом ГУАП, в срок не позднее 10 дней до даты защиты. Рецензент в срок, не превышающий 5 календарных дней, проводит анализ ВКР и предоставляет письменную рецензию на нее. В рецензии отмечается рекомендуемая оценка за выполненную работу. Наличие в рецензии неудовлетворительной оценки не является препятствием для проведения защиты такой ВКР.

Выпускающая кафедра представляет студенту на ознакомление отзыв и рецензию не позднее 5 календарных дней до предполагаемой даты защиты.

После получения рецензии студент формирует электронный вариант ВКР, отзыва и рецензии, которые должны быть полностью идентичны бумажному варианту, и передает их на выпускающую кафедру. Установлены следующие требования к электронному варианту ВКР:

- это должен быть один файл формата PDF с установленной защитой от копирования;
- файл должен иметь имя формата ГОД_МЕСЯЦ_№ГРУППЫ_ФамилияИО.pdf (например, 2021_06_3645_ИвановИИ.pdf);
- файл должен содержать текст ВКР и сканированные копии титульного листа, листа задания, отзыва руководителя и рецензии.

В соответствии с законодательством РФ в тексте ВКР не должны присутствовать производственные, технические, экономические, организационные и другие сведения, в том числе о результатах интеллектуальной деятельности в научно-технической сфере, о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность. В случае отсутствия таких сведений руководитель ВКР в своем отзыве должен написать фразу *«В работе не содержится информация с ограниченным доступом, и отсутствуют сведения, представляющие коммерческую ценность»*.

ВКР, отзыв и рецензия передаются в ГЭК не позднее, чем за два календарных дня до защиты ВКР. Дополнительно студент может передать и другие материалы, характеризующие научную и/или практическую значимость работы (печатные труды, программные продукты, макеты, акты о внедрении и др.).

После положительной защиты текст ВКР, отзыв и рецензия в бумажном варианте студент должен передать в библиотеку ГУАП на хранение, что является необходимым условием для подписания обходного листа в библиотеке.

В таблице 3 приведены основные этапы и контрольные даты процесса подготовки дипломной работы специалиста.

Таблица 3 – Этапы подготовки ВКРС

№ п.п.	Содержание этапа	Период	Форма отчета
1	Выбор и утверждение темы ВКР и дипломного руководителя	От 6 до 2 месяцев до предполагаемой даты защиты	Приказ об утверждении тем ВКР
2	Получение задания на разработку ВКР от руководителя	В течение недели с момента утверждения темы	Задание на выполнение ВКР
3	Написание ВКР, консультации с руководителем	Весь период дипломного	Полный текст ВКР

		проектирования с консультированием по согласованному с руководителем ВКР расписанием	
4	Прохождение процедуры предзащиты на кафедре	Примерно за 25-30 дней до даты защиты	Готовый текст ВКР
5	Проверка работы на объем заимствований: отправка работы	Не позднее 20 дней до даты защиты	Текст ВКР без титульного листа, содержания и списка литературы в формате pdf
	получение результата	Не позднее 15 дней до даты защиты	Отчет об объеме заимствований
6	Получение отзыва руководителя: отправка работы	Не позднее 15 дней до даты защиты	Готовый текст ВКР и отчет об объеме заимствований
	получение отзыва	Не позднее 10 дней до даты защиты	Отзыв руководителя ВКР
7	Получение рецензии: отправка работы	Не позднее 10 дней до даты защиты	Готовый текст ВКР и отзыв руководителя
	получение рецензии	Не позднее 5 дней до даты защиты	Рецензия
8	Подготовка полного комплекта ВКР	Не позднее 2 дней до даты защиты	Электронный и бумажный варианты ВКР, отзыва и рецензии
9	Передача ВКР в библиотеку на хранение	После положительной защиты ВКР	Бумажный вариант ВКР, отзыва и рецензии

6 ПОРЯДОК ПОДАЧИ И РАССМОТРЕНИЯ АПЕЛЛЯЦИИ ПО РЕЗУЛЬТАТАМ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

Порядок подачи и рассмотрения апелляции по результатам ГИА осуществляется в соответствии с требованиями РДО ГУАП. СМК 2.75 – Положение «Проведение в ГУАП государственной итоговой аттестации по образовательным программам высшего образования – программам бакалавриата, программам специалитета и программам магистратуры».

7 ПЕРЕЧЕНЬ РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ ДЛЯ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

7.1. Основная литература

Перечень основной литературы, необходимой при подготовке к ГИА, приведен в таблице 3.

Таблица 3 – Перечень основной литературы

Шифр/URL адрес	Библиографическая ссылка	Количество экземпляров в библиотеке (кроме электронных экземпляров)
004 Б 24	Баранова, Е. К. Моделирование системы защиты информации. Практикум : учебное пособие / Е. К. Баранова, А. В. Бабаш. - 2-е изд., перераб. и доп. - М. : РИОР : ИНФРА-М, 2018. - 224 с.	5
004 Б 90	Бузов, Г. А. Защита информации ограниченного доступа от утечки по техническим каналам / Г. А. Бузов. - М. : Горячая линия - Телеком, 2017. - 586 с.	5
004 Б 39	Беззатеев, Сергей Валентинович (д-р техн. наук, доц.). Программирование задач по обеспечению информационной безопасности : лабораторный практикум / С. В. Беззатеев, С. Г. Фомичева ; С.-Петербург. гос. ун-т аэрокосм. приборостроения. - Санкт-Петербург : Изд-во ГУАП, 2020. - 89 с.	5
004.056 М 87	Мошак, Николай Николаевич (д-р техн. наук, доц.). Защита информационных систем : учебно-методическое пособие / Н. Н. Мошак ; С.-Петербург. гос. ун-т аэрокосм. приборостроения. - Санкт-Петербург : Изд-во ГУАП, 2020. - 154 с.	5
004.9 Б 19	Бакай, Ксения Александровна. Основы информационной безопасности : учебное пособие / К. А. Бакай ; С.-Петербург. гос. ун-т аэрокосм. приборостроения. - Санкт-Петербург : Изд-во ГУАП, 2020. - 133 с.	5
004 Т 23	Татарникова, Татьяна Михайловна (проф.). Анализ данных в прикладных задачах обеспечения информационной безопасности : монография / Т. М. Татарникова ; С.-Петербург. гос. ун-т аэрокосм. приборостроения. - СПб. : Изд-во ГУАП, 2018. - 115 с.	5
004 И 98	Ищейнов, В. Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации : учебное пособие / В. Я. Ищейнов, М. В. Мецатунян. - 2-е изд., перераб. и доп. - М. : ФОРУМ : ИНФРА-М, 2017. - 256 с.	5

7.2. Дополнительная литература

Перечень дополнительной литературы для использования при подготовке к ГИА приведен в таблице 4.

Таблица 4 – Перечень дополнительной литературы

Шифр/URL адрес	Библиографическая ссылка	Количество экземпляров в библиотеке (кроме электронных экземпляров)
004 З-40	Защита информации : учебное пособие / А. П. Жук [и др.]. - 2-е изд. - М. : РИОР : ИНФРА-М, 2017. - 392 с.	5
338 К 22	Карзаева, Н. Н. Основы экономической безопасности : учебник / Н. Н. Карзаева. - М. : ИНФРА-М, 2019. - 275 с.	5
004 О-35	Овчинников, Андрей Анатольевич (канд. техн. наук, доц.). Основы информационной безопасности. Исторические шифры : учебно-методическое пособие / А. А. Овчинников ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - СПб. : Изд-во ГУАП, 2018. - 40 с.	5
004 Ш 22	Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. - М. : ДМК Пресс, 2017. - 702 с.	5
004.4 И 46	Ильина, Дарья Викторовна. Проектирование и разработка безопасных веб-приложений : учебное пособие / Д. В. Ильина ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - Санкт-Петербург : Изд-во ГУАП, 2019. - 43 с.	5

8 РЕСУРСЫ ИНФОРМАЦИОННО–ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ»

Перечень ресурсов информационно–телекоммуникационной сети «Интернет», необходимых при подготовке к ГИА, представлен в таблице 5.

Таблица 5 – Перечень ресурсов информационно–телекоммуникационной сети «Интернет», необходимых при подготовке к ГИА

URL адрес	Наименование
www.intuit.ru	Национальный Открытый Университет "ИНТУИТ"
www.znaniy.com	Электронная библиотечная система
www.e.lanbook.com	Электронная библиотечная система

9 МАТЕРИАЛЬНО–ТЕХНИЧЕСКАЯ БАЗА

Перечень материально–технической базы, необходимой для проведения ГИА,

представлен в таблице 6.

Таблица 6 – Материально–техническая база

№ п/п	Наименование материально–технической базы	Номер аудитории (при необходимости)
1	Специализированная мебель; технические средства обучения, служащие для представления учебной информации большой аудитории; переносной набор демонстрационного оборудования	190000, РФ, г. Санкт-Петербург, ул. Большая Морская, д. 67, лит. А, пом. 42Н-125Н, Л6-Л20 Ауд. 13-15

10 ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

10.1. Фонд оценочных средств для проведения ГЭ.

10.1.1. Состав фонда оценочных средств приведен в таблице 7.

Таблица 7 – Состав фонда оценочных средств для проведения ГЭ

Форма проведения ГЭ	Перечень оценочных средств
Письменная	Список вопросов к экзамену

10.1.2. Перечень компетенций, освоение которых оценивается на ГЭ, приведен в таблице 2 раздела 4 программы ГИА.

10.1.3. Описание показателей и критериев для оценки компетенций, а также шкал оценивания для ГЭ.

Описание показателей для оценки компетенций для ГЭ:

- способность последовательно, четко и логично излагать материал программы дисциплины;
- умение справляться с задачами;
- умение формулировать ответы на вопросы в рамках программы ГЭ с использованием материала научно–методической и научной литературы;
- уровень правильности обоснования принятых решений при выполнении практических задач.

Оценка уровня сформированности (освоения) компетенций осуществляется на основе таких составляющих как: знание, умение, владение навыками и/или опытом деятельности в соответствии с требованиями ФГОС по освоению компетенций для соответствующей ОП.

В качестве критериев оценки уровня сформированности (освоения) у студентов компетенций при проведении ГЭ в формах «устная» и «письменная» применяется 4–балльная

шкала, а при проведении ГЭ с применением средств электронного обучения применяется 100–балльная шкала (таблица 8).

Таблица 8 –Критерии оценки уровня сформированности компетенций

Оценка компетенции		Характеристика сформированных компетенций
100–балльная шкала	4–балльная шкала	
$85 \leq K \leq 100$	«отлично»	– студент глубоко и всесторонне усвоил учебный материал образовательной программы (ОП); – уверенно, логично, последовательно и грамотно его излагает; – опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения к практической деятельности направления; – умело обосновывает и аргументирует выдвигаемые им идеи; – делает выводы и обобщения; – свободно владеет системой специализированных понятий.
$70 \leq K \leq 84$	«хорошо»	– студент твердо усвоил учебный материал образовательной программы, грамотно и по существу излагает его, опираясь на знания основной литературы; – не допускает существенных неточностей; – увязывает усвоенные знания с практической деятельностью направления; – аргументирует научные положения; – делает выводы и обобщения; – владеет системой специализированных понятий.
$55 \leq K \leq 69$	«удовлетворительно»	– студент усвоил только основной учебный материал образовательной программы, по существу излагает его, опираясь на знания только основной литературы; – допускает несущественные ошибки и неточности; – испытывает затруднения в практическом применении знаний направления; – слабо аргументирует научные положения; – затрудняется в формулировании выводов и обобщений; – частично владеет системой специализированных понятий.
$K \leq 54$	«неудовлетворительно»	– студент не усвоил значительной части учебного материала образовательной программы; – допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении; – испытывает трудности в практическом применении знаний; – не может аргументировать научные положения; – не формулирует выводов и обобщений.

10.1.4. Типовые контрольные задания или иные материалы

Список вопросов и/или задач для проведения ГЭ в письменной/устной форме представлены в таблицах 9 – 10. Тесты для ГЭ, проводимого с применением средств электронного обучения, представлены в таблице 11.

Таблица 9 – Список вопросов для ГЭ, проводимого в письменной/устной форме

№ п/п	Список вопросов для ГЭ, проводимого в письменной/устной форме	Компетенции
1.	Цели, задачи и принципы построения комплексных систем защиты информации	ОК-1, ОК-3, ОК-5, ОК-7, ОК-8, ОПК-1
2.	Цели и задачи защиты информации в автоматизированных системах.	ОК-2, ОК-3, ОК-5, ОК-7, ОК-8, ОПК-1
3.	Методологические основы организации комплексных систем защиты информации	ОК-1, ОК-3, ОК-5, ОК-7, ОК-8, ОПК-1
4.	Разработка политики безопасности предприятия.	ОК-2, ОК-3, ОК-5, ОК-7, ОК-8, ОПК-1
5.	Требования, предъявляемые к комплексным системам защиты информации	ОК-2, ОК-3, ОК-5, ОК-7, ОК-8, ОПК-1
6.	Состав, объекты и степень конфиденциальности защищаемой информации.	ОК-2, ОК-3, ОК-5, ОК-7, ОК-8, ОПК-1
7.	Методика выявления состава носителей защищаемой информации.	ОК-2, ОК-3, ОК-5, ОК-7, ОК-8, ОПК-1
8.	Факторы, определяющие необходимость защиты периметра и здания предприятия.	ОК-1, ОК-3, ОК-5, ОК-7, ОК-8, ОПК-1
9.	Особенности помещений как объектов защиты для работы по защите информации.	ОК-2, ОК-3, ОК-5, ОК-7, ОК-8, ОПК-1
10.	Состав средств обеспечения, подлежащих защите.	ОК-2, ОК-3, ОК-5, ОК-7, ОК-8, ОПК-1
11.	Факторы, создающие угрозу информационной безопасности.	ОК-2, ОК-3, ОК-5, ОК-7, ОК-8, ОПК-1
12.	Угрозы безопасности информации.	ОК-2, ОК-3, ОК-5, ОК-7, ОК-8, ОПК-1
13.	Модели нарушителей безопасности АС.	ОК-2, ОК-3, ОК-5, ОК-7, ОК-8, ОПК-1
14.	Обеспечение безопасности информации в непредвиденных ситуациях.	ОК-2, ОК-3, ОК-5, ОК-7, ОК-8, ОПК-1
15.	Технические каналы утечки информации, их классификация.	ОК-2, ОК-3, ОК-5, ОК-7, ОК-8, ОПК-1
16.	Особенности защиты речевой информации.	ОК-2, ОК-3, ОК-5, ОК-7, ОК-8, ОПК-1

17.	Механизмы обеспечения безопасности информации.	ОК-2, ОК-3, ОК-5, ОК-7, ОК-8, ОПК-1
18.	Методика выявления нарушителей, тактики их действий и состава интересующей их информации.	ОК-1, ОК-3, ОК-5, ОК-7, ОК-8, ОПК-1
19.	Особенности синтеза СЗИ АС от НСД.	ОК-4, ОК-5, ОК-7, ОК-8, ОПК-1
20.	Методика синтеза СЗИ.	ОК-4, ОК-5, ОК-7, ОК-8, ОПК-1
21.	Оптимальное построение системы защиты для АС.	ОК-4, ОК-5, ОК-7, ОК-8, ОПК-1
22.	Проектирование системы защиты информации для существующей АС.	ОК-4, ОК-5, ОК-7, ОК-8, ОПК-1
23.	Общая характеристика задач моделирования КСЗИ.	ОК-2, ОК-3, ОК-5, ОК-7, ОК-8, ОПК-1
24.	Формальные модели безопасности и их анализ.	ОК-2, ОК-3, ОК-5, ОК-7, ОК-8, ОПК-1
25.	Прикладные модели защиты информации в АС.	ОК-2, ОК-3, ОК-5, ОК-7, ОК-8, ОПК-1
26.	Формализация модели безопасности.	ОК-2, ОК-3, ОК-5, ОК-7, ОК-8, ОПК-1
27.	Показатель уровня защищенности, основанный на экспертных оценках.	ОК-2, ОК-3, ОК-5, ОК-7, ОК-8, ОПК-1
28.	Методы проведения экспертного опроса.	ОК-2, ОК-3, ОК-5, ОК-7, ОК-8, ОПК-2
29.	Экономический подход к оценке эффективности комплексных систем защиты информации	ОК-2, ОК-3, ОК-5, ОК-7, ОК-8, ОПК-2
30.	Основные понятия и определения криптографии.	ОК-5, ОК-7, ОК-8, ОПК-2
31.	Виды криптосистем. Задачи, решаемые методами криптографии.	ОК-4, ОК-5, ОК-7, ОК-8, ОПК-2
32.	Виды информации, подлежащие закрытию, их модели и свойства. Частотные характеристики открытых сообщений. Критерии на открытый текст. Особенности нетекстовых сообщений.	ОК-4, ОК-5, ОК-7, ОК-8, ОПК-2
33.	История криптографии. Основные этапы становления науки криптографии.	ОК-4, ОК-5, ОК-7, ОК-8, ОПК-2
34.	Классификация шифров замены. Шифр Цезаря. Шифр простой замены. Шифр Плейфера. Полибианский квадрат. Шифр Хилла. Шифр Виженера. Частотный анализ. Тест Казиски.	ОК-4, ОК-5, ОК-7, ОК-8, ОПК-2
35.	Классификация шифров перестановки. Примеры шифров перестановки и их криптоанализ.	ОК-4, ОК-5, ОК-7, ОК-8, ОПК-2
36.	Шифры гаммирования. Шифр Вернама. Подходы к его	ОК-4, ОК-5, ОК-

	криптоанализу.	7, ОК-8, ОПК-2
37.	Композиции шифров. Enigma. Шифр Хейглина.	ОК-4, ОК-5, ОК-7, ОК-8, ОПК-2
38.	Математическая модель шифра.	ОК-4, ОК-5, ОК-7, ОК-8, ОПК-2
39.	Атаки и угрозы шифрам.	ОК-4, ОК-5, ОК-7, ОК-8, ОПК-2
40.	Блочные шифры и их ключевая система. Замены и перестановки.	ОК-4, ОК-5, ОК-7, ОК-8, ОПК-2
41.	Сеть Файстеля. Шифры DES, ГОСТ 28147-89.	ОК-4, ОК-5, ОК-7, ОК-8, ОПК-2
42.	Шифр AES	ОК-4, ОК-5, ОК-7, ОК-8, ОПК-2
43.	Шифр IDEA.	ОК-4, ОК-5, ОК-7, ОК-8, ОПК-2
44.	Подходы к криптоанализу блочных шифров. Дифференциальный криптоанализ. Линейный криптоанализ.	ОК-4, ОК-5, ОК-7, ОК-8, ОПК-2
45.	Этапы разработки программного обеспечения. Постановка задачи и спецификация программы.	ОК-1, ОК-5, ОК-7, ОК-8, ОПК-2
46.	Анализ требований, предъявляемых к программе.	ОК-3, ОК-5, ОК-7, ОК-8, ОПК-2
47.	Проектирование программы. Кодирование. Отладка и тестирование. Эксплуатация и сопровождение.	ОК-3, ОК-5, ОК-7, ОК-8, ОПК-2
48.	Анализ требований к программе. Содержание и порядок составления спецификаций. Диалоговые программы. Дружественность, жизненный цикл программы.	ОК-3, ОК-5, ОК-7, ОК-8, ОПК-2
49.	Постановка задачи и спецификация программы. Выбор алгоритма.	ОК-3, ОК-5, ОК-7, ОК-8, ОПК-4
50.	Особенности программирования математических формул. Структурное программирование.	ОК-3, ОК-5, ОК-7, ОК-8, ОПК-4
51.	Способы конструирования программ. Модульные программы. Нисходящая разработка.	ОК-4, ОК-5, ОК-7, ОК-8, ОПК-4
52.	Пошаговая детализация. Псевдокод и блок-схемы.	ОК-4, ОК-5, ОК-7, ОК-8, ОПК-4
53.	Программирование рекурсивных алгоритмов.	ОК-4, ОК-5, ОК-7, ОК-8, ОПК-4
54.	Полный набор типов данных. Стандартные типы данных. Представление основных структур программирования. Типы данных, определяемые пользователем.	ОК-4, ОК-5, ОК-7, ОК-8, ОПК-4
55.	Перечисляемые и ограниченные типы данных. Символьные типы. Массивы. Тип множество. Процедурный тип. Типы данных, определяемые пользователем.	ОК-4, ОК-5, ОК-7, ОК-8, ОПК-4
56.	Записи. Файлы. Динамический тип данных	ОК-4, ОК-5, ОК-7, ОК-8, ОПК-4
57.	Списки. Программирование рекурсивных алгоритмов. Способы конструирования программ. Модульные программы	ОК-4, ОК-5, ОК-7, ОК-8, ОПК-4
58.	Определение операций над типами, определяемыми пользователем. Слабая. и сильная типизация языков программирования	ОК-4, ОК-5, ОК-7, ОК-8, ОПК-4

59.	Указатели и динамические структуры данных. Списки. Абстрактные структуры данных.	ОК-3, ОК-5, ОК-7, ОК-8, ОПК-4
60.	Использование ссылок и надежность программ.	ОК-3, ОК-5, ОК-7, ОК-8, ОПК-4
61.	Основы доказательства правильности. Процесс производства программных продуктов. Основные подходы. Процедурное, логическое, функциональное и объектно-ориентированное программирование.	ОК-3, ОК-5, ОК-7, ОК-8, ОПК-4
62.	Методы, технология и инструментальные средства.	ОК-3, ОК-5, ОК-7, ОК-8, ОПК-4
63.	Обзор современных языков программирования. Выбор языка. Общие требования к организации программы. Выбор имен. Комментарии. Форматирование программы. Организация ввода-вывода	ОК-1, ОК-5, ОК-7, ОК-8, ОПК-4
64.	Оптимизация программы. Стиль записи программы, форматирование и программы-форматеры.	ОК-4, ОК-5, ОК-7, ОК-8, ОПК-4
65.	Конструирование вложенных условных операторов. Использование процедур и функций при разработке программ. Применение рекурсии.	ОК-4, ОК-5, ОК-7, ОК-8, ОПК-4
66.	Область применения ООП. Определение объектов. Область действия полей объекта и параметр SELF. Наследование. Присваивание объектов. Полиморфизм. Динамические объекты.	ОК-4, ОК-5, ОК-7, ОК-8, ОПК-4
67.	Создание и освобождение объектов. Обработка ошибок при работе с динамическими объектами. Модули, экспортирующие объекты.	ОК-4, ОК-5, ОК-7, ОК-8, ОПК-4
68.	Основы доказательства правильности. Тестирование и отладка. Различие между отладкой и тестированием.	ОК-1, ОК-5, ОК-7, ОК-8, ОПК-4
69.	Надежность программ и защитное программирование. Тестирование программ и технические требования к тестам. Методы отладки.	ОК-3, ОК-5, ОК-7, ОК-8, ОПК-4
70.	Обзор характерных ошибок и их обнаружение. Использование отладчиков. Планирование испытаний программы. Оценка полноты проверки программы.	ОК-3, ОК-5, ОК-7, ОК-8, ОПК-4
71.	Документирование и стандартизация. Проектирование программного обеспечения. Руководство по техническому обслуживанию. Правила внесения изменений.	ОК-1, ОК-5, ОК-7, ОК-8, ОПК-4
72.	Требования к документированию государственного стандарта ЕСПД. Необходимый набор документов.	ОК-3, ОК-5, ОК-7, ОК-8, ПК-1
73.	Руководства пользователя и системного программиста.	ОК-3, ОК-5, ОК-7, ОК-8, ПК-1
74.	Коммутационная подсистема РИС	ОК-3, ОК-5, ОК-7, ОК-8, ПК-1
75.	Подсистемы РИС	ОК-3, ОК-5, ОК-7, ОК-8, ПК-1
76.	Особенности защиты информации в РИС	ОК-3, ОК-5, ОК-7, ОК-8, ПК-1
77.	Корпоративные и общедоступные РИС.	ОК-3, ОК-5, ОК-7, ОК-8, ПК-1
78.	Проблемы защиты информации в РИС	ОК-3, ОК-5, ОК-7, ОК-8, ПК-1

79.	Проблемы проектирования реляционных БД.	ОК-3, ОК-5, ОК-7, ОК-8, ПК-1
80.	Модели структурного проектирования. Метод структурного анализа и проектирования	ОК-3, ОК-5, ОК-7, ОК-8, ПК-1
81.	Защита информации в БД	ОК-3, ОК-5, ОК-7, ОК-8, ПК-1
82.	Базы данных. СУБД. Классификация	ОК-3, ОК-5, ОК-7, ОК-8, ПК-1
83.	Типология БД. Документальные БД. Фактографические БД	ОК-3, ОК-5, ОК-7, ОК-8, ПК-1
84.	Типология БД. Гипертекстовые и мультимедийные БД	ОК-3, ОК-5, ОК-7, ОК-8, ПК-1
85.	Объектно-ориентированные БД	ОК-3, ОК-5, ОК-7, ОК-8, ПК-1
86.	Типология БД. Распределенные БД. Коммерческие БД	ОК-3, ОК-5, ОК-7, ОК-8, ПК-1
87.	Иерархическая и сетевая модели данных	ОК-3, ОК-5, ОК-7, ОК-8, ПК-1
88.	Элементы реляционной модели данных	ОК-3, ОК-5, ОК-7, ОК-8, ПК-1
89.	Реляционное исчисление. Организация процессов обработки данных в БД. Ограничения целостности	ОК-3, ОК-5, ОК-7, ОК-8, ПК-1
90.	Построение системы защиты информации в РИС.	ОК-1, ОК-5, ОК-7, ОК-8, ПК-1
91.	Особенности защиты информации от непреднамеренных угроз в РИС	ОК-4, ОК-5, ОК-7, ОК-8, ПК-1
92.	Пример разработки ER-модели.	ОК-4, ОК-5, ОК-7, ОК-8, ПК-1
93.	Хранение отношений. Организация индексов.	ОК-4, ОК-5, ОК-7, ОК-8, ПК-1
94.	Транзакции. Сериализация транзакций.	ОК-4, ОК-5, ОК-7, ОК-8, ПК-1
95.	Жизненный цикл БД. Модели жизненного цикла ПО	ОК-4, ОК-5, ОК-7, ОК-8, ПК-1
96.	Принципы построения БД. Нормальные формы.	ОК-4, ОК-5, ОК-7, ОК-8, ПК-1
97.	Принципы построения БД. Метод «Сущность-связь».	ОК-4, ОК-5, ОК-7, ОК-8, ПК-1

Таблица 10 – Перечень задач для ГЭ, проводимого в письменной/устной форме

№ п/п	Перечень задач для ГЭ, проводимого в письменной/устной форме	Компетенции
	Не предусмотрено	

Таблица 11 – Тесты для ГЭ, проводимого с применением средств электронного обучения

№ п/п	Тесты для ГЭ, проводимого с применением средств электронного обучения	Компетенции
	Не предусмотрено	

10.2. Фонд оценочных средств для оценки защиты ВКР

10.2.1. Описание показателей и критериев для оценки компетенций, а также шкал оценивания для ВКР и ее защиты.

Описание показателей для оценки компетенций для ВКР и ее защиты:

- актуальность темы ВКР;
- научная обоснованность предложений и выводов;
- использование производственной информации и методов решения инженерно–технических, организационно–управленческих и экономических задач;
- теоретическая и практическая значимость результатов работы и/или исследования;
- полнота и всестороннее раскрытие темы ВКР;
- соответствие результатов работы и/или исследования поставленным цели и задачам в ВКР;
- соответствие оформления ВКР установленным требованиям;
- умение четко и ясно доложить содержание ВКР;
- умение обосновать и отстаивать принятые решения;
- умение отвечать на поставленные вопросы;
- знание передового отечественного и зарубежного опыта;
- уровень самостоятельности выполнения работы и обоснованность объема цитирования;
- другое (уровень экономического обоснования, знание законодательных и нормативных документов, методических материалов по вопросам, касающимся конкретного направления).

Оценка уровня сформированности (освоения) компетенций осуществляется на основе таких составляющих как: знание, умение, владение навыками и/или опытом деятельности в соответствии с требованиями ФГОС по освоению компетенций для соответствующей ОП.

В качестве критериев оценки уровня сформированности (освоения) у студента компетенций применяется 4–балльная шкала, представленная в таблице 12.

Таблица 12 –Критерии оценки уровня сформированности компетенций

Оценка компетенции (4–балльная шкала)	Характеристика сформированных компетенций
«отлично»	– студент глубоко и всесторонне усвоил учебный материал ОП, уверенно, логично, последовательно и грамотно его излагает; – опираясь на знания основной и дополнительной литературы, студент свободно привязывает усвоенные научные положения к практической деятельности, обосновывая выдвинутые

	предложения; – студент умело обосновывает и аргументирует выбор темы ВКР и выдвигаемые им идеи; – студент аргументировано делает выводы; – прослеживается четкая корреляционная зависимость между поставленными целью и задачами и полученными результатами работы и/или исследования; – студент свободно владеет системой специализированных понятий; – содержание доклада, иллюстративно–графического материала (при наличии) студента полностью соответствует содержанию ВКР; – студент соблюдает требования к оформлению ВКР и иллюстративно–графического материала (при наличии); – студент четко выделяет основные результаты своей профессиональной деятельности и обосновывает их теоретическую и практическую значимость; – студент строго придерживается регламента выступления; – студент ясно и аргументировано излагает материалы доклада; – присутствует четкость в ответах студента на поставленные членами государственной экзаменационной комиссии (ГЭК) вопросы; – студент точно и грамотно использует профессиональную терминологию при защите ВКР.
«хорошо»	– студент всесторонне усвоил учебный материал ОП, логично, последовательно и грамотно его излагает; – опираясь на знания основной и дополнительной литературы, студент привязывает усвоенные научные положения к практической деятельности, обосновывая выдвинутые предложения; – студент грамотно обосновывает выбор темы ВКР и выдвигаемые им идеи; – студент обоснованно делает выводы; – прослеживается зависимость между поставленными целью и задачами и полученными результатами работы и/или исследования; – студент владеет системой специализированных понятий; – содержание доклада и иллюстративно–графического материала (при наличии) студента соответствует содержанию ВКР; – студент соблюдает требования к оформлению ВКР и иллюстративно–графического материала (при наличии); – студент выделяет основные результаты своей профессиональной деятельности и обосновывает их теоретическую и практическую значимость; – студент придерживается регламента выступления; – студент ясно излагает материалы доклада; – присутствует логика в ответах студента на поставленные членами ГЭК вопросы; – студент грамотно использует профессиональную терминологию при защите ВКР.
«удовлетворительно»	– студент слабо усвоил учебный материал ОП, при его изложении допускает неточности;

	– опираясь на знания только основной литературы, студент привязывает научные положения к практической деятельности направления, выдвигая предложения; – студент слабо и неуверенно обосновывает выбор темы ВКР и выдвигаемые им идеи; – студент не аргументировано делает выводы и заключение; – не прослеживается зависимость между поставленными целью и задачами и полученными результатами работы и/или исследования; – студент плохо владеет системой специализированных понятий; – содержание доклада и иллюстративно–графического материала (при наличии) студента не полностью соответствует содержанию ВКР; – студент допускает ошибки при оформлении ВКР и иллюстративно–графического материала (при наличии); – студент слабо выделяет основные результаты своей профессиональной деятельности и не обосновывает их теоретическую и практическую значимость; – студент отступает от регламента выступления; – студент сбивчиво и не уверенно излагает материалы доклада; – отсутствует логика в ответах студента на поставленные членами ГЭК вопросы; – студент не точно использует профессиональную терминологию при защите ВКР.
«неудовлетворительно»*	– студент не усвоил учебный материал ОП, при его изложении допускает неточности; – допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении; – студент не может обосновать выбор темы ВКР; – студент не может сформулировать выводы; – слабая зависимость между поставленными целью и задачами и полученными результатами работы и/или исследования; – студент не владеет системой специализированных понятий; – содержание доклада и иллюстративно–графического материала (при наличии) студента не полностью соответствует содержанию ВКР; – студент не соблюдает требования к оформлению ВКР и иллюстративно–графического (при наличии) материала; – студент не выделяет основные результаты своей профессиональной деятельности и не может обосновать их теоретическую и практическую значимость; – студент не соблюдает регламент выступления; – отсутствует аргументированность при изложении материалов доклада; – отсутствует ясность в ответах студента на поставленные членами ГЭК вопросы; – студент не грамотно использует профессиональную терминологию при защите ВКР; – содержание ВКР не соответствует установленному уровню оригинальности.

* *Примечание: оценка неудовлетворительно ставится, если ВКР и ее защита не удовлетворяют большинству перечисленных в таблице 12 критериев.*

10.2.2. Перечень тем ВКР

Перечень тем ВКР на текущий учебный год, предлагаемый студентам, приводится в Приложении № 1.

10.2.3. Уровень оригинальности содержания ВКР составляет не менее «70» %.

10.3. Методические материалы, определяющие процедуры оценивания результатов освоения ОП.

В качестве методических материалов, определяющих процедуру оценивания результатов освоения ОП, используются:

- МДО ГУАП. СМК 3.165 – «Методические рекомендации о разработке фонда оценочных средств образовательных программ высшего образования»;
- РДО ГУАП. СМК 2.75 – Положение «Проведение в ГУАП государственной итоговой аттестации по образовательным программам высшего образования – программам бакалавриата, программам специалитета и программам магистратуры»;
- РДО ГУАП. СМК 2.76 – Положение «Порядок разработки, оформления и утверждения программы государственной итоговой аттестации по образовательным программам высшего образования – программам бакалавриата, программам специалитета и программам магистратуры»;
- РДО ГУАП. СМК 3.160 – Положение «О выпускной квалификационной работе студентов ГУАП, обучающихся по образовательным программам высшего образования – программам бакалавриата, программам специалитета и программам магистратуры»;
- а также методические материалы выпускающей кафедры, определяющие процедуру оценивания результатов освоения ОП, не противоречащих локальным нормативным актам ГУАП.

Перечень тем ВКР, предлагаемый студентам

1. Организация безопасного удаленного доступа к ЛВС предприятия (название предприятия).
2. Построение защищенной виртуальной сети на базе специализированного программного обеспечения на предприятии (название предприятия).
3. Автоматизация учета конфиденциальных документов на предприятии (название предприятия).
4. Организация процессов мониторинга конфиденциального документооборота на предприятии (название предприятия).
5. Автоматизация процесса проверок наличия конфиденциальных документов на предприятии (название предприятия).
6. Разработка комплексной системы защиты информации (КСЗИ) предприятия (название предприятия).
7. Организация системы планирования и контроля функционирования КСЗИ на предприятии (название предприятия).
8. Разработка основных направлений совершенствования КСЗИ предприятия (наименование предприятия).
9. Организация подсистемы, обеспечивающей управление КСЗИ в условиях чрезвычайной ситуации на предприятии (наименование предприятия).
10. Разработка методологии проектирования КСЗИ.
11. Разработка моделей процессов защиты информации при проектировании КСЗИ.
12. Анализ методов оценки качества функционирования КСЗИ.
13. Разработка структурно-функциональной модели управления КСЗИ предприятия (наименование предприятия).
14. Разработка проекта программно-аппаратной защиты информации предприятия (наименование предприятия).
15. Разработка методов расчета экономической эффективности программно-аппаратной защиты информации предприятия (наименование предприятия).
16. Криптографические средства защиты информации на основе дискретных носителей.
17. Разработка игровой (дискретной) модели программно-аппаратной защиты информации предприятия (наименование предприятия).
18. Разработка изолированной программно-аппаратной среды в Windows NT (WINDOWS 2000, LINUX и т.д.) (наименование предприятия).
19. Обоснование и разработка требований и процедур по защите информации ограниченного доступа на предприятии (название предприятия).
20. Обоснование и разработка мер организационной защиты конфиденциальной информации при взаимодействии сотрудников предприятия со сторонними организациями (название предприятия).
21. Разработка методов и форм работы с персоналом предприятия, допущенным к конфиденциальной информации (название предприятия).
22. Обоснование и разработка требований и процедур по защите конфиденциальной информации, обрабатываемой средствами вычислительной техники и информационными системами (название предприятия).
23. Организация порядка установления внутриобъектного режима на объекте информатизации (название предприятия).
24. Организация защиты персональных данных (название предприятия).
25. Разработка и анализ эффективности внедрения мер по защите информации объектов, подключенных к глобальной сети (название предприятия).
26. Защита информации в банковской сфере

27. Разработка организационно-технических мероприятий по обеспечению безопасности функционирующей информационно-вычислительной системы при вводе в эксплуатацию (внедрении) ее дополнительных очередей (подсистем) сторонними организациями (название предприятия).

28. Разработка типового проекта комплексной системы защиты информации на предприятии (название предприятия).

29. Разработка типового проекта комплексной системы защиты информации (название предприятия).

30. Проект комплексной системы защиты информации (название предприятия) с разработкой системы видеонаблюдения.

31. Проект комплексной системы защиты информации (название предприятия) с разработкой системы охрано-пожарной системы.

32. Проект комплексной системы защиты информации (название предприятия) с разработкой защищенной системы связи.

33. Проект комплексной системы защиты информации (название предприятия) с разработкой виброакустической защиты выделенного помещения.

34. Проект защиты информации (название предприятия) с разработкой системы защиты выделенного помещения от ПЭМИН.

35. Разработка и обоснование требований и процедур по защите конфиденциальной информации, обрабатываемой средствами вычислительной техники.

36. Программные модели каналов утечки информации с объекта защиты.

37. Криптографические методы защиты на основе избыточности информации.

38. Разработка методов передачи и защиты информации в каналах связи.

39. Разработка защищенной БД на предприятии.

Лист внесения изменений в программу ГИА

Дата внесения изменений и дополнений. Подпись внесшего изменения	Содержание изменений и дополнений	Дата и № протокола заседания кафедры	Подпись зав. кафедрой