МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования
"САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ"

Кафедра № 33

УТВЕРЖДАЮ
Ответственный за образовательную программу

доц.,к.э.н.,доц.
(должность, уч. степень, звание)

Т.Н. Елина
(инициалы, фамилия)

(подпись)
«27» июня 2024 г

ПРОГРАММА ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

Код направления подготовки/ специальности	10.04.01
Наименование направления подготовки/ специальности	Информационная безопасность
Наименование направленности	Технологии искусственного интеллекта в информационной безопасности
Форма обучения	очная
Год приема	2024

Санкт-Петербург –2024

Лист согласования программы

Программу составил (а)

доц.,к.э.н.,доц.	27.06.2024	Т.Н. Елина
(должность, уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Программа одобрена на заседании кафедры № 33
«27» июня 2024 г, протокол № 11

Заведующий кафедрой № 33

д.т.н.,доц.	27.06.2024	С.В. Беззатеев
(уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Заместитель директора института №3 по методической работе

	27.06.2024	Н.В. Решетникова
(должность, уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования
"САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ"

Кафедра № 33

УТВЕРЖДАЮ
Ответственный за образовательную программу

доц.,к.э.н.,доц.

(должность, уч. степень, звание)

Т.Н. Елина

(инициалы, фамилия)

(подпись)
«27» июня 2024 г

ПРОГРАММА ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

Код направления подготовки/ специальности	10.04.01
Наименование направления подготовки/ специальности	Информационная безопасность
Наименование направленности	Технологии искусственного интеллекта в информационной безопасности
Форма обучения	очная
Год приема	2024

Санкт-Петербург –2024

Лист согласования программы

Программу составил (а)

доц.,к.э.н.,доц.	27.06.2024	Т.Н. Елина
(должность, уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Программа одобрена на заседании кафедры № 33

«27» июня 2024 г, протокол № 11

Заведующий кафедрой № 33

д.т.н.,доц.	27.06.2024	С.В. Беззатеев
(уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Заместитель директора института №3 по методической работе

	27.06.2024	Н.В. Решетникова
(должность, уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

1. ЦЕЛИ, ЗАДАЧИ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

1.1. Целью ГИА обучающихся по направлению подготовки 10.04.01 «Информационная безопасность», направленности «Технологии искусственного интеллекта в информационной безопасности», является установление уровня подготовки обучающихся к выполнению профессиональных задач и соответствия его подготовки, требуемой по ОП квалификации: магистр.

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):

Таблица 1 – Перечень компетенций и индикаторов их достижения

Категория (группа) компетенции	Код и наименование компетенции	Код и наименование индикатора достижения компетенции
Универсальные компетенции	*УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.З.1 знать методы критического анализа и системного подхода; методики разработки стратегии действий для выявления и решения проблемных ситуаций УК-1.З.2 знать цифровые ресурсы, инструменты и сервисы, включая интеллектуальные, для решения задач/проблем профессиональной деятельности УК-1.У.1 уметь искать нужные источники информации; анализировать, сохранять и передавать информацию с использованием цифровых средств; вырабатывать стратегию действий для решения проблемной ситуации УК-1.В.1 владеть навыками системного и критического мышления; методиками постановки цели, определения способов ее достижения УК-1.В.2 владеть навыками использования алгоритмов и цифровых средств, предназначенных для анализа информации и данных
Универсальные компетенции	*УК-2 Способен управлять проектом на всех этапах его	УК-2.З.1 знать этапы жизненного цикла проекта;

	жизненного цикла	виды ресурсов и ограничений для решения проектных задач; необходимые для осуществления проектной деятельности правовые нормы и принципы управления проектами УК-2.З.2 знать цифровые инструменты, предназначенные для разработки проекта/решения задачи; методы и программные средства управления проектами УК-2.У.1 уметь определять целевые этапы, основные направления работ; объяснять цели и формулировать задачи, связанные с подготовкой и реализацией проекта УК-2.У.2 уметь выдвигать альтернативные варианты действий с целью выработки новых оптимальных алгоритмов действий по проекту УК-2.В.1 владеть навыками управления проектом на всех этапах его жизненного цикла УК-2.В.2 владеть навыками решения профессиональных задач в условиях цифровизации общества
Универсальные компетенции	*УК-3 Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	УК-3.З.1 знать методики формирования команды; методы эффективного руководства коллективом; основные теории лидерства и стили руководства УК-3.З.2 знать цифровые средства, предназначенные для взаимодействия с другими людьми и выполнения командной работы УК-3.У.1 уметь

		вырабатывать командную стратегию для достижения поставленной цели; использовать цифровые средства, предназначенные для организации командной работы УК-3.В.1 владеть навыками организации командной работы; разрешения конфликтов и противоречий при деловом общении на основе учета интересов всех сторон УК-3.В.2 владеть навыками использования цифровых средств, обеспечивающих удаленное взаимодействие членов команды
Универсальные компетенции	*УК-4 Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	УК-4.З.1 знать правила и закономерности личной и деловой устной и письменной коммуникации; современные коммуникативные технологии на русском и иностранном(ых) языке(ах) УК-4.З.2 знать современные технологии, обеспечивающие коммуникацию и кооперацию в цифровой среде УК-4.У.1 уметь применять на практике технологии коммуникации и кооперации для академического и профессионального взаимодействия, в том числе в цифровой среде, для достижения поставленных целей УК-4.В.1 владеть навыками межличностного делового общения на русском и иностранном(ых) языке(ах) с применением

		современных технологий и цифровых средств коммуникации
Универсальные компетенции	*УК-5 Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	УК-5.З.1 знать правила и технологии эффективного межкультурного взаимодействия УК-5.У.1 уметь взаимодействовать с представителями иных культур с соблюдением этических и межкультурных норм УК-5.В.1 владеть навыками межкультурного взаимодействия при выполнении профессиональных задач
Универсальные компетенции	*УК-6 Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки	УК-6.З.1 знать основные принципы профессионального и личностного развития с учетом особенностей цифровой экономики и требований рынка труда; способы совершенствования своей деятельности на основе самооценки и образования УК-6.У.1 уметь определять и реализовывать приоритеты совершенствования собственной деятельности на основе самооценки, в том числе с использованием цифровых средств; решать задачи собственного личностного и профессионального развития УК-6.В.1 владеть навыками решения задач самоорганизации и собственного личностного и профессионального развития на основе самооценки, самоконтроля, в том числе с использованием цифровых средств
Общепрофессиональные	*ОПК-1 Способен обосновывать	ОПК-1.З.1 знать основы

компетенции	требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	отечественных и зарубежных стандартов в области обеспечения информационной безопасности ОПК-1.З.2 знать направления развития и проблемы компьютерного моделирования сложных систем; направления развития технологий проектирования информационных, автоматизированных и автоматических систем, и систем искусственного интеллекта ОПК-1.З.3 знать современную нормативную базу и ГОСТы, регламентирующие процесс разработки ТЗ; правила, способы и методы организации совместных разработок ОПК-1.З.4 знать методы проектирования и построения систем информационной безопасности, включая методы тестирования эффективности и оценки надёжности ОПК-1.У.1 уметь проектировать информационные системы с учетом различных технологий обеспечения информационной безопасности, в том числе систем искусственного интеллекта ОПК-1.У.2 уметь обосновывать и планировать состав и архитектуру моде-лируемых сложных систем; обосновывать и планировать состав и архитектуру проектируемых

		информационных, автоматизиро-ванных и автоматических систем и систем искусственного интеллекта ОПК-1.У.3 уметь формировать актуальную модель угроз для АИС и учитывать её положения при формировании требований ТЗ на проектируемую систему обеспечения ИБ ОПК-1.У.4 уметь разрабатывать и обосновывать критерии оценки эффективности проектируемой системы обеспечения ИБ; оценивать эффективность решений и анализировать показатели деятельности ОПК-1.У.5 уметь обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности ОПК-1.В.1 владеть навыками участия в разработке системы обеспечения информационной безопасности объекта ОПК-1.В.2 владеть навыками разработки концептуальных стратегий решения задач моделирования и проектирования автоматизированных информационных систем и систем обеспечения ИБ ОПК-1.В.3 владеть навыками планирования и оценки трудоёмкости проекта, включая техническое, кадровое и финансовое обеспечение, принятие совместных

		решений
Общепрофессиональные компетенции	*ОПК-2 Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности	ОПК-2.З.1 знать методы концептуального проектирования технологий обеспечения информационной безопасности ОПК-2.З.2 знать направления развития и проблемы компьютерного моделирования сложных систем; направления развития технологий проектирования информационных, автоматизированных и автоматических систем ОПК-2.З.3 знать современные методы и средства тестирования ОПК-2.З.4 знать принципы построения и функционирования современных информационных систем ОПК-2.З.5 знать назначение комплексной системы защиты информации, принципы ее организации и этапы разработки ОПК-2.З.6 знать требования к системам комплексной защиты информации ОПК-2.У.1 уметь выбирать и обосновывать преимущества методов решения задач для защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью ОПК-2.У.2 уметь разрабатывать тестовые планы и сценарии тестирования разработанного продукта ОПК-2.У.3 уметь управлять коллективом

		исполнителей и принимать управленческие решения ОПК-2.У.4 уметь проектировать подсистемы безопасности информационных систем с учетом действующих нормативных и методических документов ОПК-2.У.5 уметь разрабатывать модели угроз и нарушителей информационной безопасности информационных систем ОПК-2.В.1 владеть навыками выполнения работы по осуществлению при изготовлении, монтаже, наладке, испытаниях и сдаче в эксплуатацию систем и средств обеспечения информационной безопасности ОПК-2.В.2 владеть навыками практической реализации типовых задач разработки и исследования систем защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасности ОПК-2.В.3 владеть средствами автоматизированного и ручного функционального тестирования ОПК-2.В.4 владеть навыками участия в организации комплексной системы защиты объекта
Общепрофессиональные компетенции	*ОПК-3 Способен разрабатывать проекты организационнораспорядительных документов по обеспечению информационной безопасности	ОПК-3.З.1 знать основы отечественных и зарубежных стандартов в области сертификации и аттестации объектов информатизации, в области управления

		информационной безопасностью с целью разработки проектов организационно-распорядительных документов ОПК-3.З.2 знать правила создания технического задания на создание подсистем безопасности информационных систем ОПК-3.З.3 знать основные угрозы безопасности информации и модели нарушителя в информационных системах ОПК-3.З.4 знать основные нормативные правовые акты в области обеспечения информационной безопасности ОПК-3.З.5 знать нормативные методические документы ФСБ России в области защиты информации ОПК-3.З.6 знать нормативные методические документы ФСТЭК России в области информационной безопасности ОПК-3.У.1 уметь разрабатывать технические задания на создание подсистем обеспечения информационной безопасности ОПК-3.У.2 уметь проводить выбор, исследовать эффективность, проводить технико-экономическое обоснование проектных решений в области построения систем обеспечения информационной безопасности ОПК-3.У.3 уметь

		разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации ОПК-3.У.4 уметь разрабатывать нормативно-методические материалы по регламентации системы организационной защиты информации ОПК-3.У.5 уметь разрабатывать организационно-распорядительную документацию по обеспечению информационной безопасности ОПК-3.У.6 уметь работать с технической и эксплуатационной документацией ОПК-3.У.7 уметь оценивать различные инструменты в области проектирования и управления информационной безопасности ОПК-3.В.1 владеть навыками разработки политик безопасности различных уровней ОПК-3.В.2 владеть навыками расчета и управления рисками информационной безопасности, навыками разработки положения о применимости механизмов контроля в контексте управления рисками информационной безопасности ОПК-3.В.3 владеть правилами построения оптимальной политики безопасности в соответствии с требованиями уровня безопасности, стоимости и

		сроков реализации ОПК-3.В.4 владеть навыками работы с нормативными правовыми актами в области информационной безопасности
Общепрофессиональные компетенции	*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-4.З.1 знать способы формулирования научной проблемы, гипотезы, выбора предмета, объекта, целей, задач исследования ОПК-4.З.10 знать виды отчетно-информационных документов, методы их подготовки ОПК-4.З.11 знать основные теоретико-числовые методы применительно к задачам защиты информации ОПК-4.З.2 знать основные принципы создания эскизного, технического, рабочего проектов ОПК-4.З.3 знать методы анализа и обоснования выбора решений по обеспечению требуемого уровня безопасности информационных систем ОПК-4.З.4 знать современные достижения науки в области информационной безопасности ОПК-4.З.5 знать правила, способы и методы организации, выполнения и представления результатов научного исследования ОПК-4.З.6 знать о правилах и стандартах разработки отчетной документации ОПК-4.З.7 знать основные категории и понятия информационно аналитической работы, принципы и методы ее ведения

		ОПК-4.З.8 знать методы выработки и принятия информационного решения ОПК-4.З.9 знать технологии поиска, изучения, обобщения и систематизации научной информации ОПК-4.У.1 уметь составлять пошаговый план научной деятельности, проводить предпроектные исследования ОПК-4.У.2 уметь работать с научной литературой, отбирать информацию по теме научного исследования, систематизировать, классифицировать полученную информацию ОПК-4.У.3 уметь определять комплекс мер для обеспечения безопасности информационных систем, составлять аналитические обзоры по вопросам обеспечения информационной безопасности систем ОПК-4.У.4 уметь использовать методы и средства анализа защищенности информационных систем ОПК-4.У.5 уметь использовать программные и аппаратные средства персонального компьютера для поиска и обработки информации ОПК-4.У.6 уметь разрабатывать планы и программы проведения научных исследований в соответствии с техническим заданием, ресурсным обеспечением и

		заданными сроками выполнения работы ОПК-4.У.7 уметь представлять результаты научно-исследовательской деятельности в виде презентаций, отчетов, устных докладов ОПК-4.У.8 уметь логически мыслить, вести научные дискуссии ОПК-4.У.9 уметь использовать справочную и научную литературу по тематике решаемых информационных задач, оценивать специальную информацию, систематизировать ее, принимать решение о ее дальнейшем использовании ОПК-4.В.1 владеть навыками структурирования информации по теме исследования ОПК-4.В.2 владеть навыками самостоятельного научного мышления, обобщения и систематизации информации ОПК-4.В.3 владеть навыками сбора и обработки информации в глобальной компьютерной сети, в том числе в мультидисциплинарных реферативных базах данных Scopus, Web of Knowledge ОПК-4.В.4 владеть методикой создания технического задания и технического проекта при организации НИОКР ОПК-4.В.5 владеть программными и программно-аппаратными средствами анализа систем

		защиты информации ОПК-4.В.6 владеть навыками поиска информации в глобальной информационной сети Интернет ОПК-4.В.7 владеть методологией научных исследований в сфере информационной безопасности ОПК-4.В.8 владеть навыками планирования научного исследования ОПК-4.В.9 владеть основными методами поиска и структурирования информации
Общепрофессиональные компетенции	*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	ОПК-5.З.1 знать теоретические и эмпирические методы научных исследований ОПК-5.З.10 знать основные элементы научно-технического эксперимента ОПК-5.З.11 знать приемы выбора основных факторов эксперимента и технологию построения факторных планов ОПК-5.З.12 знать требования ГОСТов на оформление научно-технической документации ОПК-5.З.13 знать современные модели и методы измерения, прогнозирования, принятия решений при решении практических задач ОПК-5.З.14 знать принципы построения вероятностных моделей применительно к практическим задачам ОПК-5.З.2 знать порядок проведения научных исследований ОПК-5.З.3 знать методику

		проведения патентных исследований, объектом которых могут являться объекты техники, промышленной и интеллектуальной собственности (изобретения, полезные модели, программы для ЭВМ и базы данных и др.), ноу-хау и пр. ОПК-5.З.4 знает порядок организации процесса исследования эффективности системы управления ИБ ОПК-5.З.5 знать нормативные и методические материалы в сфере информационной безопасности ОПК-5.З.6 знать принципы организации технического, программного и информационного обеспечения информационной безопасности ОПК-5.З.7 знать методы построения оптимальных планов для научных экспериментов ОПК-5.З.8 знать правила, способы и методы организации, выполнения и представления результатов научного исследования ОПК-5.З.9 знать принципы построения и функционирования современных информационных систем ОПК-5.У.1 уметь применять методы научных исследований в научной деятельности, в частности, при написании магистерской диссертации и научных статей ОПК-5.У.2 уметь составлять отчеты о

		патентных исследованиях по ГОСТ ОПК-5.У.3 умеет формализовать задачи анализа безопасности информационных систем, разрабатывать методики исследования и применять инструментальные средства анализа безопасности ОПК-5.У.4 уметь составлять и корректировать план проведения работ в зависимости от полученных результатов ОПК-5.У.5 уметь оформлять и представлять результаты, полученные в ходе выполнения научно-исследовательского проекта грамотно, лаконично, в достаточном объеме на русском и иностранном языках ОПК-5.У.6 уметь выбирать и применять в профессиональной деятельности экспериментальные и расчетно-теоретические методы исследований ОПК-5.У.7 уметь работать со специальными программным средствами для оформления проектной и отчетной документации ОПК-5.У.8 уметь обобщать полученные экспериментальные данные, анализировать и делать выводы ОПК-5.В.1 владеть навыками оформления научных публикаций в соответствие с шаблоном IEEE, требованиями научных конференций ОПК-5.В.10 владеть навыками самостоятельной работы,

		самоорганизации ОПК-5.В.2 владеть теоретическими и эмпирическими методами научного исследования при выполнении научно-исследовательских работ ОПК-5.В.3 владеть методикой оформления отчетов по научно-исследовательским работам согласно ГОСТ ОПК-5.В.4 владеет навыками выбора и обоснования критериев оценки защищенности открытых информационных систем ОПК-5.В.5 владеет навыками обработки, оценки и представления результатов исследования эффективности решений по управлению информационной безопасностью ОПК-5.В.6 владеть навыками разработки технической документации в соответствии с требованиями Единой системы конструкторской документации и Единой системы программной документации ОПК-5.В.7 владеть навыками анализа получаемых результатов и формулировки выводов ОПК-5.В.8 владеть навыками формирования и аргументированного обоснования собственной позиции по различным проблемам защиты информации ОПК-5.В.9 владеть навыками представления результатов работы в виде презентаций, пояснительных записок, научных докладов и статей

Профессиональные компетенции	*ПК-1 Способен проводить исследования по оценке уровня безопасности компьютерных систем и сетей	ПК-1.З.1 знает уязвимости информационных систем, в том числе систем искусственного интеллекта ПК-1.У.1 умеет анализировать информационную систему с ис-кусственным интеллектом с целью определе-ния уровня защищен-ности и доверия ПК-1.В.1 владеет оценкой рисков, связанных с осуществлением угроз безопасности в от-ношении информаци-онных систем
Профессиональные компетенции	*ПК-2 Способен обосновывать перспективы проведения исследований в области интеллектуальной защиты объектов информатизации	ПК-2.З.1 знает методы, средства и практику планирования, организации, проведения и внедрения научных исследований и опытно-конструкторских разработок ПК-2.У.1 умеет анализировать новую научную проблематику в области интеллекту-альной защиты объектов информатизации ПК-2.В.1 владеет навыками проведения анализа новых направлений исследований в области интеллектуальной защиты объектов информатизации
Профессиональные компетенции	*ПК-3 Способен проводить научно-исследовательские и опытно-конструкторские работы в сфере создания защищённых телекоммуникационных систем	ПК-3.З.1 знает национальные, межгосударственные и международные стандарты, устанавливающие требования к организации и проведению научно-исследовательских, опытно-конструкторских работ, опытной эксплуатации средств и систем защиты электросетей

		ПК-3.У.1 умеет планировать этапы выполнения НИОКР по созданию средств и систем защиты электросетей ПК-3.В.1 владеет организацией подготовки отчетных документов по итогам проведения НИОКР в соответствии с нормативными документами и требованиями заказчика
Профессиональные компетенции	*ПК-4 Способен разрабатывать средства и системы защиты сетей электросвязи от несанкционированного доступа, а также защищённых телекоммуникационных систем	ПК-4.З.1 знает методы, способы, средства, последовательность и содержание этапов разработки средств и систем защиты сетей от НСД, защищённых телекоммуникационных систем ПК-4.У.1 умеет разрабатывать проекты, технические задания, планы и графики проведения работ по защите сетей от НСД и необходимую техническую документацию ПК-4.В.1 владеет разработкой предложений и практической реализацией элементов, средств и систем защиты сетей от НСД, а также защищённых телекоммуникационных систем, включая разработку программного обеспечения
Профессиональные компетенции	*ПК-5 Способен разрабатывать требования по защите и формировать политики безопасности компьютерных систем и сетей	ПК-5.З.1 знает виды политик безопасности компьютерных систем и сетей ПК-5.У.1 умеет формулировать задания по безопасности компьютерных систем ПК-5.В.1 владеет разработкой профилей

		защиты и заданий по безопасности
Профессиональные компетенции	*ПК-6 Способен проводить контрольные проверки работоспособности и эффективности применяемых средств защиты информа-ции	ПК-6.З.1 знает методы и методики оценки безопасности программно-аппаратных средств защиты информации ПК-6.У.1 умеет применять разработанные методики оценки защищенности программно-аппаратных средств защиты информации ПК-6.В.1 владеет оценкой работоспособности и эффективности применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик
Профессиональные компетенции	*ПК-7 Способен проводить анализ угроз информационной безопасности в сетях электросвязи	ПК-7.З.1 знает организационно-технические мероприятия по обеспечению защиты сетей электросвязи от НСД и их эффективность ПК-7.У.1 умеет проводить проверку работоспособности и эффективности применяемых программноаппаратных (в том числе криптографических) и технических средств защиты сетей электросвязи от НСД ПК-7.В.1 владеет выработкой предложений по предотвращению и нейтрализации угроз НСД к сетям электросвязи

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

2. ФОРМЫ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

ГИА проводится в форме:

- подготовка к сдаче и сдача государственного экзамена(ГЭ);
- выполнение и защита выпускной квалификационной работы (ВКР).

3. ОБЪЕМ И ПРОДОЛЖИТЕЛЬНОСТЬ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

Объем и продолжительность ГИА указаны в таблице 2.

Таблица 2 – Объем и продолжительность ГИА

№ семестра	Трудоемкость ГИА (ЗЕ)	Продолжительность в неделях
4	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 3.1.

Таблица 3.1 – Перечень компетенций, уровень освоения которых оценивается на ГЭ

УК-1 «Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий»
Производственная практика (научно-исследовательская работа)
Производственная практика
Теория множественного доступа
Теория систем и системный анализ
Технологии обеспечения информационной безопасности
Производственная преддипломная практика
УК-2 «Способен управлять проектом на всех этапах его жизненного цикла»
Производственная практика (научно-исследовательская работа)
Производственная практика
Коммерциализация результатов научных исследований и разработок
Производственная преддипломная практика
УК-3 «Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели»
Коммерциализация результатов научных исследований и разработок
Производственная практика
Производственная преддипломная практика
УК-4 «Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия»
Иностранный язык (профессиональный)
УК-5 «Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия»
Иностранный язык (профессиональный)
Методология и организация научных исследований
Производственная практика
Производственная преддипломная практика
УК-6 «Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки»
Методология и организация научных исследований
Научно-технический семинар
ОПК-1 «Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание»

Защищенные информационные системы
Технологии обеспечения информационной безопасности
Производственная преддипломная практика
ОПК-2 «Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности»
Защищенные информационные системы
Технологии обеспечения информационной безопасности
Управление информационной безопасностью
Производственная преддипломная практика
ОПК-3 «Способен разрабатывать проекты организационнораспорядительных документов по обеспечению информационной безопасности»
Технологии обеспечения информационной безопасности
Управление информационной безопасностью
Производственная преддипломная практика
ОПК-4 «Способен осуществлять сбор, обработку и анализ научно- технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок»
Методология и организация научных исследований
Теория информации
Защищенные информационные системы
Технологии обеспечения информационной безопасности
Управление информационной безопасностью
Производственная преддипломная практика
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»
Методология и организация научных исследований
Теория информации
Защищенные информационные системы
Технологии обеспечения информационной безопасности
Управление информационной безопасностью
Производственная преддипломная практика
ПК-1 «Способен проводить исследования по оценке уровня безопасности компьютерных систем и сетей»
Программно-аппаратные средства защиты информации в инфокоммуникационных системах и сетях
Производственная практика (научно-исследовательская работа)
Теоретические основы компьютерной безопасности
Анализ защищенности компьютерных систем
ПК-2 «Способен обосновывать перспективы проведения исследований в области интеллектуальной защиты объектов информатизации»
Производственная практика (научно-исследовательская работа)
Методы машинного обучения
Специальные разделы математики
Теория игр и исследование операций
ПК-3 «Способен проводить научно-исследовательские и опытно-конструкторские работы в сфере создания защищённых телекоммуникационных систем»
Научно-технический семинар
Производственная практика (научно-исследовательская работа)
ПК-4 «Способен разрабатывать средства и системы защиты сетей электросвязи от несанкционированного доступа, а также защищённых телекоммуникационных систем»

Сотовые сети
Теоретические основы компьютерной безопасности
Производственная практика
Теория множественного доступа
Теория построения инфокоммуникационных систем и сетей
Теория систем и системный анализ
Безопасность баз данных
Виртуальные частные сети
Постквантовая криптография
ПК-5 «Способен разрабатывать требования по защите и формировать политики безопасности компьютерных систем и сетей»
Анализ защищенности компьютерных систем
ПК-6 «Способен проводить контрольные проверки работоспособности и эффективности применяемых средств защиты информа-ции»
Методы моделирования и оптимизации
Программно-аппаратные средства защиты информации в инфокоммуникационных системах и сетях
Квантовая криптография
Математические основы постквантовой криптографии
ПК-7 «Способен проводить анализ угроз информационной безопасности в сетях электросвязи»
Теоретические основы компьютерной безопасности
Специальные разделы физики
Криптология
Постквантовая криптография
Производственная практика

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. ГЭ проводится для студентов, допущенных к ГИС, в соответствии с утвержденным расписанием.

ГЭ проводится по нескольким дисциплинам ОП, результаты освоения которых имеют определяющее значении для профессиональной деятельности выпускников.

ГЭ проводится в письменной форме в период после завершения преддипломной практики и завершается аттестационной оценкой «отлично», «хорошо», «удовлетворительно», «неудовлетворительно», оформляется протоколов 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. Перед ГЭ проводится консультирование студентов по вопросам, включенным в программу ГИА.

В период подготовки в ГЭ обучающемуся рекомендуется подготовить обстоятельные ответы согласно списку вопросов, выносимых на ГЭ, используя при необходимости рекомендуемую для подготовки к ГЭ литературу, а также посетить консультации, проводимые перед ГЭ.

Ответы обучающегося должны продемонстрировать глубокое и всестороннее усвоение учебного материала образовательно 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 (или ссылка на отдельный документ при наличии).

Во время проведения государственного экзамена в письменной форме в аудитории должно находиться не менее двух членов ГЭК. 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.

Проверка письменной работы каждого студента, сдающего государственный экзамен, осуществляется комиссией в составе не менее двух третей от состава ГЭК.

Результаты государственных аттестационных испытаний, проводимых в письменной форме, объявляются секретарем ГЭК студентам не позднее следующего рабочего дня после проведения государственного аттестационного испытания.

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.

5. ТРЕБОВАНИЯ К ВЫПУСКНЫМ КВАЛИФИКАЦИОННЫМ РАБОТАМ И ПОРЯДКУ ИХ ВЫПОЛНЕНИЯ

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

Порядок выбора темы ВКР, требования к структуре и объему ВКР, содержанию основных разделов, оформлению текста ВКР, иллюстративно-графического материала, требования к подготовке и защите ВКР, а также рекомендации для студентов по докладу на защите ВКР и порядок проведения защиты представлены в методических указаниях [37 И 74] «Информационная безопасность». Выпускная квалификационная работа: методические указания / С.-Петерб. гос. ун-т аэрокосм. приборостроения; сост.:Е.А. Крук, А.А. Овчинников, – СПб. : Изд-во ГУАП, 2017. – 31 с.

5.2. Дополнительные компоненты ВКР определяемые выпускающей кафедрой.

Определения, обозначения и сокращения

В данный раздел должны быть включены определения специфических терминов, используемых в ВКР. А также в случае использования в тексте значительного количества сокращений и условных обозначений, необходимо привести их расшифровки.

Сокращения русских слов выполняются в соответствии с ГОСТ 7.0.12-2011, иностранных – ГОСТ 7.11-2004.

Общепринятые сокращения, установленные в национальных стандартах и соответствующие правилам орфографии русского языка, допускается приводить без расшифровки.

Пример

т.е. – то есть; и т.д. – и так далее; и др. – и другое; г. – год, с. – страница и др.

Недопустимо использовать следующие сокращения:

- сокращения слов, не установленных правилами орфографии русского языка;
- сокращения единиц физических величин, если они употребляются без числовых значений, не в таблицах и не на рисунках.

Введение

Введение является обязательным разделом ВКР, оно должно включать следующие сведения:

1) актуальность темы работы;
2) цель и задачи работы;
3) краткое описание объекта и предмета исследования;
4) характеристику структуры работы.

Заключение

Заключение является обязательным разделом ВКР, оно должно включать следующие сведения:

1) перечень результатов работы;
2) практическую значимость или научную новизну полученных результатов;
3) используемые в работе методы и средства достижения результатов.

В заключении не должно содержаться цитат и прочих текстовых заимствований.

Список использованных источников

Можно использовать заголовки:

1) Список использованной литературы
2) Список использованных источников
3) Библиографический список
4) Библиография

Список использованных источников должен содержать библиографическое описание всех литературных источников, использованных в процессе выполнения ВКР. Список необходимо оформлять в соответствии с требованиями ГОСТ Р 7.0.100-2018 и ГОСТ 7.82-2001.

Каждый источник использованной литературы должен содержать информацию об авторе материала, если он есть. Также нужно отразить название материала, сведения о редакторе и переводчике (если издание иноязычное).

Указывают и тип издания (оно может быть повторное, переработанное, дополненное). Также прописываются год издания и количество страниц.

Нумерация списка выполняется арабскими цифрами (не римскими, не точками, не буквами). Страница списка использованных источников обязательно нумеруется и включается в оглавление.

Порядок сортировки источников должен быть следующим:

- международные нормативные акты;
- конституция Российской Федерации;
- нормативно-правовые документы:
    - Федеральные конституционные законы
    - Постановления конституционного суда
    - Кодексы
    - Федеральные законы

    - Законы
    - Указы Президента РФ
    - Акты Правительства
        - Постановления
        - Распоряжения
- Акты Верховного и Высшего Арбитражного Судов.
- Нормативные акты министерств и ведомств
    - Постановления
    - Приказы
    - Распоряжения
    - Письма
- Региональные нормативные акты
- ГОСТы
- СНиПы, СП, ЕНИРы, ТУ
- книги, учебные пособия, статьи, монографии, электронные источники (CD-диски, ссылки из Интернета)
- иностранные источники.

Список использованных источников в каждом подразделе может составляться:

- в порядке цитирования (упоминания в работе);
- в хронологическом порядке (в порядке опубликования книги или документов);
- в алфавитном порядке;
- в систематическом порядке (по научным направлениям).

Приложения

Приложения к дипломной работе по специальностям 10.04.01 могут содержать:

- модели бизнес-процессов, потоков данных и инфологические модели;
- должностные инструкции персонала;
- экономические расчеты и графики;
- листинг программного кода;
- юридические документы;
- шаблоны форм и отчетов;
- акты внедрения;
- другие инструкции, методики, алгоритмы, разработанные в процессе выполнения ВКР.

Приложения включаются в общую нумерацию страниц ВКР. Все приложения должны быть перечислены в содержании с указанием их буквенных обозначений, заголовков и номеров страниц, с которых они начинаются.

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 10.04.01 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 студентов 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 проводится 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.

Защита ВКР (за исключением работ, содержащих сведения, составляющие государственную тайну) проводится на открытом заседании ГЭК с участием не менее

двух третей её состава в установленное расписанием время. Кроме членов ГЭК на защите могут присутствовать другие лица: обучающиеся, представители заинтересованных предприятий, организаций, учреждений, руководители ВКР, консультанты, преподаватели и др. Председатель ГЭК имеет право удалить сторонних лиц при нарушении ими порядка проведения защиты ВКР. При проведении защиты ВКР, по решению председателя ГЭК, может проводиться видеозапись. Перед началом проведения защиты ВКР председатель ГЭК уведомляет присутствующих о проведении видеозаписи.

За день до защиты студент должен разместить на кафедральном компьютере необходимые для демонстрации своей работы материалы: презентацию, программное приложение и др.

В начале заседания председатель ГЭК знакомит студентов с порядком проведения защиты ВКР.

Перед началом защиты ВКР секретарь ГЭК представляет студента и тему его ВКР.

Защита начинается с доклада студента по теме ВКР. Структура доклада и его продолжительность должны соответствовать рекомендациям.

После завершения доклада члены ГЭК задают студенту вопросы, связанные с темой ВКР.

После ответов студента на вопросы секретарем ГЭК зачитываются отзыв руководителя ВКР и рецензия. В случае, когда руководитель ВКР и/или рецензент присутствуют на заседании, председатель ГЭК может предоставить им возможность самостоятельно зачитать свой отзыв или рецензию. После зачитывания отзыва руководителя ВКР и рецензии студенту предоставляется возможность ответа на замечания.

Члены ГЭК оценивают содержание работы и ее защиту, включающую доклад и ответы на вопросы. При выставлении оценок члены ГЭК используют критерии, приведенные в разделе 2.5.

В конце заседания в закрытом режиме ГЭК выставляет согласованные итоговые оценки по каждой проведенной защите ВКР на основании оценок членов ГЭК с учетом оценки рецензента.

Решения ГЭК оформляются протоколами и доводятся до сведения студентов в торжественной обстановке по окончании заседания ГЭК.

Целью доклада является демонстрация знания теоретических и методических положений применительно к теме работы и умения их реализовать на конкретном объекте. Во время защиты в отведенное время студент должен показать знание темы, умение логично и четко излагать материал исследования, обосновать полученные выводы, продемонстрировать уровень приобретенных компетенций.

Рекомендуемая структура доклада для специальностей 10.04.01 приведена в таблице 1.

Таблица 1 – Общая структура доклада на защите ВКРС

№ п.п.	Специальность 10.04.01
1	Актуальность темы работы
2	Цель и задачи работы
3	Результаты аналитического поиска существующих решений
4	Анализ предметной области
5	Инжиниринг/Реинжиниринг бизнес-процессов
6	Архитектура разрабатываемой системы
7	Используемые средства, методы и технологии
8	Структура базы данных

9	Вопросы информационной безопасности и защиты информации
10	Оценка эффективности предлагаемых решений
11	Выводы по работе

Желательно, чтобы доклад не зачитывался с листа. Допустимо использование распечатанного варианта доклада для ориентировки во времени выступления и содержании доклада. На защиту отводится не более 15 минут, из которых 5-7 минут занимает доклад, 3 минуты показ программного или технического продукта (при наличии), 7 минут – ответы на вопросы и замечания руководителя, рецензента и комиссии.

При подготовке доклада следует избегать сложных деепричастных оборотов, тяжелых словесных конструкций. Повествование ведется от третьего лица («в работе рассмотрено... », «было установлено, что ... » и т.п.).

Студенту необходимо заранее отрепетировать выступление вслух, провести хронометраж, проанализировать продолжительность различных частей доклада. Доклад должен быть четко структурирован: тезисы доклада должны быть выделены (принадлежность определенному слайду или плакату) для быстрого ориентирования докладчика во время защиты в соответствии со структурой иллюстративно-графического материала.

В основной части выступления (тему ВКР повторять не стоит, ее оглашает секретарь ГЭК) произносится приветственное слово членам комиссии, далее производится переход к тексту доклада. По завершению выступления необходимо выразить слова благодарности членам комиссии за внимание.

При ответах на вопросы членов ГЭК следует учитывать следующее:

1) необходимо выслушать вопрос до конца;
2) если вопрос не понят по существу или не расслышан, то целесообразно попросить повторить вопрос;
3) ответ на вопрос должен быть кратким и по существу.

После оглашения отзыва руководителя ВКР и рецензии, студент соглашается с указываемыми в них замечаниями или формулирует ответы на замечания кратко и по существу. Отвечая на вопросы, можно обращаться к тексту ВКР и/или материалам доклада, иллюстративно-графическому и другим вспомогательным материалам.

5.6. Методические указания по процедуре выполнения ВКР по направлению, определяемые выпускающей кафедрой в соответствии с локальными нормативными актами ГУАП (или ссылка на отдельный документ при наличии).

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 (рис. 2.3), 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 кафедры 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_3643_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.

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 о проведении в ГУАП государственной итоговой аттестации по образовательным программам высшего образования – программам бакалавриата, программам специалитета и программам магистратуры.

7. ПЕРЕЧЕНЬ РЕКОМЕНДУЕМЫХ ПЕЧАТНЫХ И ЭЛЕКТРОННЫХ УЧЕБНЫХ ИЗДАНИЙ ДЛЯ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

7.1. Основная литература

Перечень печатных и электронных учебных изданий, необходимых при подготовке к ГИА, приведен в таблице 4.

Таблица 4 – Перечень печатных и электронных учебных изданий

Шифр/ URL адрес	Библиографическая ссылка	Количество экземпляров в библиотеке (кроме электронных экземпляров)
37 **Г 72**	Государственная итоговая аттестация : методические указания по подготовке к государственному экзамену и написанию и защите выпускной квалификационной работы / С.-Петерб. гос. ун-т аэрокосм. приборостроения ; сост.: С. Г. Фомичева, Т. Н. Елина, В. А. Мыльников. - Санкт-Петербург : Изд-во ГУАП, 2021. - 79 с. : рис., табл. - Библиогр.: с. 79 (10 назв.). - Б. ц. - Текст : непосредственный.	5
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	5

	практикум / С. В. Беззатеев, С. Г. Фомичева ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - Санкт-Петербург : Изд-во ГУАП, 2020. - 89 с.	
004.056 **М 87**	**Мошак, Николай Николаевич** (д-р техн. наук, доц.). Защита информационных систем : учебно-методическое пособие / Н. Н. Мошак ; С.-Петерб. 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.-Петерб. 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.-Петерб. 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
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
001.8(075) **Б 79**	**Болдин, А.П.** Основы научнх исследований : учебник / А. П. Болдин, В. А. Максимов. – М.: Академия, 2012. –	20

	334 с.	
519.6/8 **М 19**	**Маликов, Р. Ф.** Основы математического моделирования : учебное пособие / Р. Ф. Маликов, - М.: Горячая линия – Телеком, 2010. – 366 с.	10
004.056.55(075) **Б 70**	Блоковые шифры : учебное пособие / С. В. Безатеев, Е. А. Крук, А. А. Овчинников, В. Б. Прохорова; С.-Петерб. гос. ун-т аэрокосм. приборостроения. – СПб. : Изд-во ГУАП, 2003. – 63 с.	9
004.056(075) **М 87**	**Мошак, Николай Николаевич** (д-р техн. наук, доц.). Защита информационных систем : учебно-методическое пособие / Н. Н. Мошак ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - Санкт-Петербург : Изд-во ГУАП, 2020. - 154 с.	5
004.056(075) **К 84**	**Крук, Е. А.** Криптография с открытым ключом. Кодовые системы : учебное пособие / Е. А. Крук, Е. М. Линский; С-Петерб. гос. ун-т аэрокосм. приборостроения – СПб. : Изд-во ГУАП, 2004. – 52 с.	22
519.81 **А 66**	**Андронов, С. А.** Модели и методы в системах поддержки принятия решений : учебное пособие / С. А. Андронов ; С-Петерб. гос. ун-т аэрокосм. приборостроения – СПб. : Изд-во ГУАП, 2008. – 176 с.	119
004.9(075) **К 95**	**Кутузов, О. И.** Математические схемы и алгоритмы моделирования инфокоммуникационных систем : учебное пособие / О. И. Кутузов, Т. М. Татарникова; С-Петерб. гос. ун-т аэрокосм. приборостроения – СПб. : Изд-во ГУАП, 20013. – 147 с.	62
004.94 **С 40**	**Сирота, А. А.** Компьютерное моделирование и оценка эффективности сложных систем : учебное пособие / А. А. Сирота. – М. : Техносфера, 2006. – 280 с.	30
004.6(075) **С 56**	**Совето, Б. Я.** Базы данных : теория и практика : учебник / Б. Я. Советов, В. В. Цехановский, В. Д. Чертовской. – 2-е изд. – М. : Юрайт, 2012. – 464 с.	60
Х404 **Л 77**	**Лопатин, В. Н.** Защита интеллектуальной собственности. Т. 3 / В. Н. Лопатин, В. В. Дорошков; ред. В. Н. Лопатин ; Респ. науч.-исслед. ин-т интеллект. собственности. – М. : Юрайт, 2010. – 343 с.	9
004.49(075) **Ш 22**	**Шаньгин, В. Ф.** Защита компьютерной информации. Эффективные методы и средства : учебное	1

	пособие / В. Ф. Шаньгин. – М. : ДМК Пресс, 2008. – 544 с.	
005.53(075) **М 59**	**Микони, С. В.** Теория принятия управленческих решений : учебное пособие / С. В. Микони. – СПб. : Лань, 2015. – 448 с.	5
621.3.047.77(075) **И 26**	**Игнатов, А. Н.** Микросхемотехника и наноэлектроника : учебное пособие / А. Н. Игнатов. – СПб. : Лань, 2011. – 528 с.	21
https://e.lanbook.com/book/167810	**Демидович, Б. П.** Численные методы анализа. Приближение функций, дифференциальные и интегральные уравнения : учебное пособие / Б. П. Демидович, И. А. Марон, Э. З. Шувалова. – 5-е изд., стер. – Санкт-Петербург : Лань, 2021. – 400 с	
https://e.lanbook.com/book/167860	**Юдович, В. И.** Математические модели естественных наук : учебное пособие / В. И. Юдович. – Санкт-Петербург : Лань, 2021. – 336 с.	
https://e.lanbook.com/book/153917	**Мазалов, В. В.** Математическая теория игр и приложения : учебное пособие для вузов / В. В. Мазалов. – 4-е изд., перераб. и доп. – Санкт-Петербург : Лань, 2021. – 500 с.	
https://e.lanbook.com/book/104440	**Петров, С. В.** Обеспечение безопасности организаций и производственных объектов : учебное пособие / С. В. Петров. – Москва : ЭНАС, 2007. – 224 с.	

8. ПЕРЕЧЕНЬ ЭЛЕКТРОННЫХ ОБРАЗОВАТЕЛЬНЫХ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ»

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

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

URL адрес	Наименование
www.intuit.ru	Национальный Открытый Университет "ИНТУИТ"
www.znanium.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	190000, РФ, г. Санкт-

	обучения, служащие для представления учебной информации большой аудитории; переносной набор демонстрационного оборудования	Петербург, ул. Большая Морская, д. 67, лит. А, пом. 42Н-125Н, Л6-Л20 Ауд. 13-15

10. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

10.1. Средства измерения индикаторов достижения компетенций, оценочные средства для проведения ГЭ.

10.1.1. Состав оценочных средств приведен в таблице 7.

Таблица 7 – Состав средств измерения индикаторов достижения компетенций, оценочные средства для проведения ГЭ

Форма проведения ГЭ	Перечень оценочных средств
Письменная	Список вопросов к экзамену Задачи

10.1.2. Перечень компетенций, освоение которых оценивается на ГЭ, приведен в таблице 3 раздела 4 программы ГИА.

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

Описание показателей для оценки индикаторов достижения 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 профессиональной деятельности в соответствии с требованиями ФГОС по освоению компетенций для соответствующей ОП.

Для оценки критериев уровня сформированности (освоения) компетенций студентами при проведении ГЭ в формах «устная» и «письменная» применяется 5-балльная шкала, которая приведена таблице 8. При проведении ГЭ с применение средств электронного обучения применяется 100-балльная шкала (таблица 8).

Таблица 8 –Шкала оценки критериев уровня сформированности компетенций

Оценка компетенции		Характеристика сформированных компетенций
5-балльная шкала	100-балльная шкала	
«отлично»	$85 \le К \le 100$	– 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 увязывает усвоенные научные положения с практической деятельностью направления; – умело обосновывает и аргументирует выдвигаемые им идеи;

		– делает выводы и обобщения; – свободно владеет системой специализированных понятий.
«хорошо»	$70 \le К \le 84$	– 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.
«удовлетвори тельно»	$55 \le К \le 69$	– 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.
«неудовлетво рительно»	$К \le 54$	– 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.		УК-1
2.		УК-2
3.	Методики формирования команды	УК-3
4.	Методы эффективного руководства коллективом	УК-3
5.		УК-4
6.	Основные правила и технологии межкультурного взамодействия	УК-5
7.		УК-6
8.	Структура и функции системы управления информационной безопасностью	ОПК-1
9.	Нормативно-технические документы аудита информационной безопасности	ОПК-1
10.	Федеральный закон о коммерческой тайне. Перечень сведений, которые не могут составлять коммерческую	ОПК-1

	тайну	
11.	Закон о государственной тайне. Указ Президента Российской Федерации об утверждении перечня сведений, отнесенных к государственной тайне	ОПК-1
12.	Этапы создания системы управления информационной безопасностью	ОПК-2
13.	Архитектура системы обеспечения информационной безопасности. Роль политики безопасности в задачах управления информационной безопасностью	ОПК-2
14.	Стандарты управления информационной безопасностью	ОПК-2
15.	Политика безопасности и ее роль в управлении информационной безопасностью	ОПК-3
16.	Методика оценки рисков информационной безопасности компании. Управление рисками	ОПК-3
17.	Нормативно-технические документы аудита информационно безопасности	ОПК-3
18.		ОПК-4
19.		ОПК-5
20.	Понятие объекта защиты информации	ПК-1
21.	Модель угроз и уязвимостей	ПК-1
22.	Оценка информационных рисков. Методы оценки рисков	ПК-1
23.	Управление рисками	ПК-1
24.	Мероприятия по снижению уровня риска	ПК-1
25.	Мероприятия для защиты информации при ее утечке через сеть электропитания	ПК-1
26.	Аппаратные и программно-аппаратные средства криптозащиты данных	ПК-1
27.		ПК-2
28.	Интенсификация сотрудничества между исследовательскими организациями, университетами и компаниями	ПК-3
29.	Применение методов алгебры в криптографических задачах	ПК-3, ПК-7
30.	Доктрина информационной безопасности Российской Федерации. Стратегия развития информационного общества в Российской Федерации	ПК-3
31.	Определение системы. Объект, предмет и задачи теории систем. Суть системного подхода	ПК-4
32.	Количественные и качественные методики управления рисками	ПК-4
33.	Системы защиты ПЭВМ от несанкционированного доступа к информации	ПК-4
34.	Виртуальные частные сети. Концепция, назначение, архитектурные решения. Способы создания ВЧС	ПК-4
35.	Концептуальные основы IPSec	ПК-4
36.	Принципы оптимизации запросов к БД	ПК-4
37.	Параллельный доступ к БД. Способы решения конфликтов	ПК-4
38.	Транзакции, блокировки, защита от отказов	ПК-4
39.	Модель безопасности с полным перекрытием	ПК-5
40.	Организационные мероприятия по защите информации в	ПК-5

	информационной системе	
41.	Критерии оценки безопасности информационных систем	ПК-5
42.	Основные преимущества и недостатки системы Crypton Sigma	ПК-6
43.	Комплексная система на базе единого персонального средства аутентификации и хранения ключевой информации	ПК-6
44.	Системы обнаружения и предотвращения компьютерных атак	ПК-6
45.	Сравнительный анализ программных и аппаратных комплексов, рассчитанных на защиту персональных ЭВМ от несанкционированного доступа к ЭВМ, которые разграничивают доступ к информации и устройствам ПЭВМ	ПК-6
46.	Мониторинг информационной безопасности. Аудит ИБ. Методы, меры и средства контроля и управления ИБ.	ПК-6
47.	Методы контроля целостности информации	ПК-7
48.	Основные методы защиты от копирования	ПК-7
49.	Защита алгоритма шифрования	ПК-7
50.	Методы противодействия дизассемблированию	ПК-7
51.	Задачи криптоанализа	ПК-7
52.	Принципы криптографии с открытым ключом. Классы сложности P, NP, NPC	ПК-7
53.	Основы линейного и дифференциального криптоанализа	ПК-7
54.	Защищенные распределенные (облачные) вычисления	ПК-7
55.	Взаимодействие серверных веб-приложений с БД	ПК-7
56.	Сессии. Ограничение доступа к содержимому веб-страниц	ПК-7
57.	Характеристика типовых задач, решаемых клиентскими программами. Функциональные возможности клиентской части	ПК-7

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

№ п/п	Перечень задач для ГЭ, проводимого в письменной форме	Компетенции
1	Задача 1. Для передачи сообщений по телеграфу каждая буква русского алфавита (Е и Ё отождествлены) представляется в виде пятизначной комбинации из нулей и единиц, соответствующих двоичной записи номера данной буквы в алфавите (нумерация букв начинается с нуля). Например, буква А представляется в виде 00000, буква Б - 00001, буква Ч - 10111, буква Я - 11111. Передача пятизначной комбинации производится по кабелю, содержащему пять проводов. Каждый двоичный разряд передается по отдельному проводу. При приеме сообщения перепутали провода, поэтому вместо переданного слова получен набор букв ЭАВЬЩО. Найдите переданное слово. Задача 2. При шифровании открытый текст разбивается	ПК-6, ПК-7

	на блоки одинаковой длины и в каждом блоке осуществляется перестановка букв по одной и той же схеме. Восстановите исходное сообщение по криптограмме. ПЬОКМРХТЮЕШИРООМОПЙОККНЩИТОИРПФАРГА Задача 3. Тридцати двум буквам русского алфавита А, Б, В, ..Э, Ю, Я приписаны соответственно числа 1, 2, 3, ..30, 31, 0 (буквы Е и Ё отождествляются). Выбрано некоторое нечетное число k (секретный ключ). Дешифрование текста осуществляется побуквенно следующим образом: 1) число a, соответствующее данной букве, умножается на k, 2) вычисляется остаток r от деления a*k на 32 3) выписывается буква, соответствующая числу r. Расшифруйте криптограммы: 1. ЕЦВ РФЗФЧНЙОЯ ЗМСФЦМ АМХХЛЭ 2. ЦОДШФДЮ ПКЫМЙМЯ 3. ЁРЪЫШРЫЪЩДБ ПЪДЛЪКООВЪДАКЩВБ Задача 4. Коммерсант для передачи цифровой информации с целью контроля передачи разбивает строчку передаваемых цифр на пятерки и после каждых двух пятерок приписывает две последние цифры от суммы чисел, изображенных этими пятерками. Затем процесс шифрования осуществляется путем прибавления к шифруемым цифрам членов арифметической прогрессии с последующей заменой сумм цифр остатками от деления на 10. Прочитайте зашифрованное сообщение: 4 2 3 4 6 1 4 0 5 3 1 3. Задача 5. Буквы русского алфавита занумерованы в соответствии с таблицей: Для зашифровки сообщения, состоящего из n букв, выбирается ключ K - некоторая последовательность из n букв приведенного выше алфавита. Шифрование каждой буквы сообщения состоит в сложении ее номера в таблице с номером соответствующей буквы ключевой последовательности и замене полученной суммы на букву алфавита, номер которой имеет тот же остаток от деления на 30, что и эта сумма. Прочтите шифрованное сообщение: РБЬНПТСИТСРРЕЗОХ, если известно, что шифрующая последовательность не содержала никаких букв, кроме А, Б и В. Задача 6. Рассмотрим модель шифра для цифрового текста, в котором каждая цифра заменяется остатком от деления значения многочлена f(x) = b(x3 + 7x7 + 3x + a) на число 10, где a, b — фиксированные натуральные числа. Выяснить, при каких значениях a и b возможно однозначное расшифрование.	

2	**1** На вход приемника поступают сигналы А и В. Из-за помех сигнала А в трех случаях из 4-х воспринимается как сигнал А и как В. Определить количество информации о воспринятом сигнале, содержащееся в поступившем сигнале, если поступления сигналов А и В на вход приемника одинаково вероятны. **2** По каналу связи передается 2 сигнала А1 и А2 с вероятностями Р(А1) = Р(А2) = 0.5. На выходе канала сигналы преобразуются в символы а1 и а2, причем из-за помех, которым одинаково подвержены сигналы А1 и А2, в передачу вносятся ошибки, так что в среднем один символ из 100 принимается неверно (а1 вместо а2 или а2 вместо а1). Определить среднее количество информации на символ, передаваемой по такому каналу. Сравните ее с количеством информации при отсутствии помех. **4** Имеется источник информации с производительность Н = 100 (бит/ед.вр.) и два канала связи, каждая из которых может передавать 70 двоичных знаков в единицу (0 или 1). Каждый двоичный знак заменяется противоположным с вероятностью 0,1. Требуется выяснить: достаточна ли пропускная способность этих каналов для передачи информации, поставляемой источником. **5** Алфавит источника = 0,1. Буквы равновероятны. Источник вырабатывает 100 букв в ед. времени. Канал связи передает 70 букв в ед. времени. С вероятностью 0,1 буквы искажается каналом. Сколько каналов нужно для передачи информации. **6**. Передаются три сообщения, вероятности которых 0,8; 0,1 и 0,1. Корреляция между ними отсутствует. Определить избыточность источника сообщения.	ПК-1

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. Средства измерения индикаторов достижения компетенций для оценки защиты ВКР.

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

Описание показателей для оценки индикаторов достижения 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, поставленной цели и задачам в ВКР;

– соответствие оформления ВКР установленным требованиям;

– умение четко и ясно изложить 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 профессиональной деятельности в соответствии с требованиями ФГОС по освоению компетенций для соответствующей ОП.

В качестве критериев оценки уровня сформированности (освоения) у студента компетенций применяется 5-балльная шкала, представленная в таблице 12.

Таблица 12 –Критерии оценки уровня сформированности компетенций

Оценка компетенции 5-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 увязывает усвоенные научные положения к практической деятельности, обосновывая выдвинутые предложения; – студент умело обосновывает и аргументирует выбор темы ВКР и выдвигаемые им идеи; – студент аргументированно 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

Оценка компетенции 5-балльная шкала	Характеристика сформированных компетенций
	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 не уверенно обосновывает выбор темы ВКР и выдвигаемые им идеи; – студент неаргументированно делает выводы и заключения; – 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 неуверенно излагает материалы доклада; – отсутствует логика в ответах студента на поставленные членами ГЭК вопросы; – студент неточно использует профессиональную терминологию при защите ВКР.

Оценка компетенции 5-балльная шкала	Характеристика сформированных компетенций
«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 неграмотно 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 должен составлять не менее «60» %.

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

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

- РДО ГУАП. СМК 2.75 Положение о проведении в ГУАП государственной итоговой аттестации по образовательным программам высшего образования – программам бакалавриата, программам специалитета и программам магистратуры»;
- РДО ГУАП. СМК 2.76 Положение о порядке 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.

Приложение № 1

Перечень тем ВКР, предлагаемый студентам

1. Методы и средства анализа состояния ОС WINDOWS в интересах получения доказательств при расследовании преступлений
2. Кодовая криптосистема на основе кодов, исправляющих пакеты ошибок
3. Реализация и исследование криптосистемы МакЭлиса
4. Безопасные системы агрегации данных в сенсорных сетях
5. Система цифровой подписи для документов в формате XML
6. Разработка методики применения HoneyWall при анализе поведения нарушителя
7. Модель и оптимизация кластера межсетевых экранов
8. Разработка защищенной сети пакетной передачи данных в системе-на-кристалле
9. Защищенные алгоритмы для систем хранения данных
10. Построение кодовой системы с открытым ключом
11. Сравнение эффективности использования преобразования Фурье, Уолша-Адамара, Хаара для задач цифровой стеганографии
12. Исследование схемы разделения секретов на основе кодов Рида-Соломона
13. Сравнительный анализ методов внедрения ЦВЗ при помощи расширения спектра

Приложение № 2

Рецензия на программу государственной итоговой аттестации по направлению подготовки 10.04.01 «Информационная безопасность» от работодателя

Рецензия на программу государственной итоговой аттестации по направлению подготовки 10.04.01 «Информационная безопасность», направленность «Интеллектуальные средства обеспечения безопасности объектов» от работодателя

Программа государственной итоговой аттестации (ГИА), представленная на рецензию, разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования (ФГОС) по направлению 10.04.01 «Информационная безопасность», соответствует областям предстоящей профессиональной деятельности выпускников, освоивших программу магистратуры по этому направлению.

В представленной программе прописаны все виды профессиональной деятельности выпускников и соответствующие им задачи; представлены требования к результатам освоения основной образовательной программы (выпускник должен обладать рядом общекультурных и профессиональных компетенций).

Итоговая государственная аттестация по направлению подготовки «Информационная безопасность» включает государственный экзамен (ГЭ) и защиту выпускной квалификационной работы (ВКР).

Программа содержит перечень компетенций, уровень освоения которых оценивается на ГЭ, а также описание показателей для оценки этих компетенций. Кроме того, программа включает в себя состав фонда оценочных средств для проведения ГЭ и список рекомендуемой литературы.

В программу включены примерная тематика и порядок утверждения тем ВКР, порядок выполнения и представления в государственную аттестационную комиссию ВКР, а также процедура ее защиты.

В программе ГИА отражена специфика направленности, связанная с интеллектуальными средствами обеспечения безопасности объектов. В частности, в список вопросов к государственному экзамену, а также в предлагаемую тематику выпускных работ включены вопросы, связанные с защитой операционных систем, сенсорными сетями, стеганографией, перспективными постквантовыми методами криптографической защиты.

Заключение рецензента

В программе ГИА, представленной на рецензию:

- Соблюдаются требования ко всем структурным элементам программы.

- Сформированная система оценки компетенций при проведении ГИА соответствует требованиям ФГОС высшего образования по направлению 10.04.01 «Информационная безопасность».

- Подготовка выпускника кафедры безопасности информационных систем УАИ по направлению 10.04.01 «Информационная безопасность» соответствует требованиям ФГОС по соответствующему направлению.

Считаю, что программа государственной итоговой аттестации способствует подготовке выпускников, готовых к работе на предприятиях и в организациях соответствующего профиля.

Рецензент
Директор департамента IT-сервисов Посохов Вячеслав Александрович

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