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

проф.,д.т.н.,доц.
(должность, уч. степень, звание)

С.В. Беззатеев
(инициалы, фамилия)

(подпись)

«27» июня 2024 г

ПРОГРАММА ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

Код направления подготовки/ специальности	10.05.03
Наименование направления подготовки/ специальности	Информационная безопасность автоматизированных систем
Наименование направленности	Безопасность открытых информационных систем
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 специальности 10.05.03 «Информационная безопасность автоматизированных систем», направленности «Безопасность открытых информационных систем», является установление уровня подготовки обучающихся 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):

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 УК-1.З.2 знать методики разработки стратегии действий для выявления и решения проблемных ситуаций УК-1.З.3 знать цифровые ресурсы, инструменты и сервисы для решения задач/проблем профессиональной деятельности УК-1.У.1 уметь осуществлять референтный поиск источников информации УК-1.У.2 уметь воспринимать, анализировать, сохранять и передавать информацию с использованием цифровых средств УК-1.У.3 уметь 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 жизненного цикла	УК-2.З.1 знать этапы жизненного цикла проекта; 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 УК-3.У.2 уметь использовать цифровые средства, предназначенные для организации командной работы УК-3.В.1 владеть навыками организации командной работы; разрешения конфликтов и поиска совместных решений 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 закономерности и особенности социально-исторического развития различных культур в этическом и философском контексте УК-5.У.1 уметь анализировать социально-исторические факты УК-5.У.2 уметь воспринимать этнокультурное многообразие общества УК-5.В.1 владеть навыками определения особенностей менталитета, обусловленных спецификой историко-культурного контекста УК-5.В.2 владеть навыками интерпретации ценностных ориентиров общества в процессе межкультурного взаимодействия
Универсальные компетенции	*УК-6 Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни	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
Универсальные компетенции	*УК-7 Способен поддерживать	УК-7.З.1 знать виды физических упражнений; роль и значение

	должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности	физической культуры в жизни человека и общества; научно-практические основы физической культуры, профилактики вредных привычек и здорового образа и стиля жизни УК-7.У.1 уметь применять на практике средства физической культуры и спорта для сохранения и укрепления здоровья и психофизической подготовки УК-7.В.1 владеть навыками организации здорового образа жизни с целью укрепления индивидуального здоровья для обеспечения полноценной социальной и профессиональной деятельности
Универсальные компетенции	*УК-8 Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов	УК-8.З.1 знать классификацию и источники чрезвычайных ситуаций природного и техногенного происхождения; причины, признаки и последствия опасностей, способы защиты от чрезвычайных ситуаций; принципы организации безопасности труда на предприятии и рационального природопользования УК-8.У.1 уметь поддерживать безопасные условия жизнедеятельности; выявлять признаки, причины и условия возникновения чрезвычайных ситуаций; оценивать вероятность возникновения потенциальной опасности техногенного и природного характера и принимать меры по ее предупреждению УК-8.В.1 владеть навыками применения основных методов защиты в условиях чрезвычайных ситуаций и военных конфликтов
Универсальные компетенции	*УК-9 Способен принимать обоснованные экономические решения в различных областях жизнедеятельности	УК-9.З.1 знать основы экономической теории, необходимые для решения профессиональных задач УК-9.У.1 уметь обосновывать принятие экономических решений, использовать методы экономического планирования для достижения поставленных целей УК-9.В.1 владеть навыками принятия обоснованных экономических решений в различных областях жизнедеятельности

Универсальные компетенции	*УК-10 Способен формировать нетерпимое отношение к коррупционному поведению	УК-10.З.1 знать действующие правовые нормы, обеспечивающие борьбу с коррупцией в различных областях жизнедеятельности; способы профилактики коррупции и формирования нетерпимого отношения к ней УК-10.У.1 уметь определять свою гражданскую позицию и нетерпимое отношение к коррупционному поведению УК-10.В.1 владеть навыками противодействия различным формам коррупционного поведения
Общепрофессиональные компетенции	*ОПК-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ОПК-1.З.1 знать современные достижения отечественной и зарубежной науки и техники в области информационных технологий и информационной безопасности ОПК-1.У.1 уметь определять значение информационных технологий и информационной безопасности для целей государства и общества ОПК-1.В.1 владеть навыками оценки и анализа необходимости внедрения средств автоматизации и информационной безопасности в процессы производства
Общепрофессиональные компетенции	*ОПК-2 Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности	ОПК-2.З.1 знать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности ОПК-2.У.1 уметь выбирать современные информационные технологии и программные средства, в том числе отечественного производства для решения задач профессиональной деятельности ОПК-2.В.1 владеть навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности
Общепрофессиональные компетенции	*ОПК-3 Способен использовать математические методы, необходимые для решения задач	ОПК-3.З.1 знать основные понятия и законы естественных наук, методы математического анализа и моделирования; основные методы теоретического и экспериментального

	профессиональной деятельности	исследования объектов, процессов и явлений ОПК-3.У.1 уметь использовать физико-математический аппарат для разработки математических моделей явлений, процессов и объектов при решении инженерных задач в профессиональной деятельности ОПК-3.У.2 уметь применять методы математического анализа и моделирования для обоснования принятия решений в профессиональной деятельности ОПК-3.В.1 владеть навыками проведения экспериментов по заданной методике и анализа их результатов
Общепрофессиональные компетенции	*ОПК-4 Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности	ОПК-4.З.1 знать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники ОПК-4.У.1 уметь применять основные физические законы и модели для решения задач профессиональной деятельности ОПК-4.В.1 владеть навыками анализа физических явлений и процессов функционирования микроэлектронной техники для решения задач профессиональной деятельности
Общепрофессиональные компетенции	*ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	ОПК-5.З.1 знать перечень основных нормативных правовых актов, стандартов и методических документов в области защиты информации и информационной безопасности ОПК-5.У.1 уметь применять нормативные акты при проектировании и разработке систем безопасности автоматизированных информационных систем и их компонентов ОПК-5.В.1 владеть навыками работы с нормативными документами, государственными и международными стандартами в области информационной безопасности и защиты информации
Общепрофессиональные компетенции	*ОПК-6 Способен при решении профессиональных задач организовывать	ОПК-6.З.1 знать методы и средства организации защиты информации ограниченного доступа ОПК-6.З.2 знать структуру и общий

	защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	состав нормативных и методических документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю ОПК-6.У.1 уметь осуществлять организацию защиты информации ограниченного доступа в соответствии с регламентирующими документами ОПК-6.В.1 владеть навыками применения нормативных правовых актов, нормативных и методических документов при организации системы защиты информации
Общепрофессиональные компетенции	*ОПК-7 Способен создавать программы на языках общего назначения, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ	ОПК-7.З.1 знать основные языки программирования и работы с базами данных, операционные системы и оболочки, современные программные среды разработки информационных систем и технологий ОПК-7.У.1 уметь решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением средств и методов программирования и с учетом основных требований информационной безопасности ОПК-7.В.1 владеть навыками использования методов программирования и стандартных прикладных программ для решения профессиональных задач в области информационной безопасности и защиты информации
Общепрофессиональные компетенции	*ОПК-8 Способен применять методы научных исследований при проведении разработок в области защиты информации в автоматизированных системах	ОПК-8.З.1 знать методы и процессы научных исследований, структуру научного знания, требования к научным разработкам ОПК-8.У.1 уметь проводить научные исследования в области информационной безопасности и защиты информации в автоматизированных информационных системах ОПК-8.В.1 владеть навыками научно-

		исследовательской работы при проектировании и моделировании систем защиты информации
Общепрофессиональные компетенции	*ОПК-9 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации	ОПК-9.З.1 знать технические и программные средства информационной безопасности, основы сетевых технологий и направления их совершенствования ОПК-9.У.1 уметь использовать современные технические, математические и программные средства для решения профессиональных задач ОПК-9.В.1 владеть современными технологиями, методами и моделями при разработке систем защиты информации
Общепрофессиональные компетенции	*ОПК-10 Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-10.З.1 знать криптографические модели и алгоритмы ОПК-10.У.1 уметь оценивать эффективность применения отдельных средств криптографической защиты информации в автоматизированных информационных системах ОПК-10.В.1 владеть методами реализации систем защиты информации с помощью криптографических алгоритмов
Общепрофессиональные компетенции	*ОПК-11 Способен разрабатывать компоненты систем защиты информации автоматизированных систем	ОПК-11.З.1 знать особенности проектирования автоматизированных информационных систем, методы и средства проектирования подсистем защиты информации, структуру и компоненты информационных систем ОПК-11.У.1 уметь проектировать и разрабатывать математическое и программное обеспечение автоматизированных информационных систем с учетом реализации требований информационной безопасности ОПК-11.В.1 Владеть навыками оценки целесообразности разработки и внедрения отдельных компонентов систем защиты информации
Общепрофессиональные компетенции	*ОПК-12 Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных	ОПК-12.З.1 знать теоретические основы построения баз данных, модели данных, принципы организации вычислительных сетей, сетевые технологии, технические средства их реализации, организации

	при разработке автоматизированных систем	и виды операционных систем ОПК-12.У.1 уметь проводить настройку операционных систем с соблюдением требований информационной безопасности, проектировать и организовывать безопасные вычислительные системы и базы данных ОПК-12.В.1 владеть навыками интеграции подсистем, учитывая требования информационной безопасности и защиты информации
Общепрофессиональные компетенции	*ОПК-13 Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем	ОПК-13.З.1 знать модели угроз и рисков информационной безопасности автоматизированных систем, методы оценки уязвимостей каналов передачи информации ОПК-13.У.1 уметь проводить тестирование информационной безопасности автоматизированных систем на основе оценки рисков реализации угроз безопасности ОПК-13.В.1 владеть навыками комплексного всестороннего анализа информационной безопасности автоматизированных информационных систем и их отдельных элементов
Общепрофессиональные компетенции	*ОПК-14 Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений	ОПК-14.З.1 знать особенности документирования процесса разработки информационных систем, правила формирования технического задания и подготовки исходных данных для реализации систем ОПК-14.У.1 уметь осуществлять разработку систем с учетом требований информационной безопасности ОПК-14.В.1 владеть навыками учета требований информационной безопасности в процессе внедрения и эксплуатации автоматизированных систем
Общепрофессиональные компетенции	*ОПК-15 Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем,	ОПК-15.З.1 знать методы и инструментальные средства администрирования и контроля систем защиты автоматизированных систем ОПК-15.У.1 уметь осуществлять мониторинг и периодический контроль функционирования средств и систем защиты информации

	инструментальный мониторинг защищенности автоматизированных систем	ОПК-15.В.1 владеть навыками использования инструментальных средств мониторинга и анализа состояния системы информационной безопасности
Общепрофессиональные компетенции	*ОПК-16 Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма	ОПК-16.З.1 знать специфику исторического познания и методы исторического анализа источников, а также способы хранения и трансляции социального исторического опыта ОПК-16.З.2 знать основные этапы, ключевые события и выдающихся деятелей истории с древности до наших дней; важнейшие достижения культуры и системы ценностей, сформировавшиеся в ходе исторического развития ОПК-16.У.1 уметь преобразовывать информацию в знание, осмысливать процессы, события и явления в их динамике и взаимосвязи, руководствуясь принципами научной объективности ОПК-16.У.2 уметь извлекать уроки из исторических событий, используя их в воспитании собственной гражданской позиции ОПК-16.У.3 уметь выражать свою гражданскую позицию, опираясь на знания в области традиционных религиозных культур и истории ОПК-16.В.1 владеть приемами ведения дискуссии и полемики, в том числе с использованием категориального аппарата истории ОПК-16.В.2 владеть навыками работы с историческими источниками; навыками реферирования, аннотирования и рецензирования научной литературы
Общепрофессиональные компетенции	*ОПК-17 Способен разрабатывать и реализовывать политику информационной безопасности открытых информационных систем	ОПК-17.З.1 знать методы защиты информационных ресурсов от возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, её носители, процессы обработки и передачи, а также минимизации рисков информационной безопасности ОПК-17.У.1 уметь выявлять,

		предупреждать и пресекать возможную противоправную и иную негативную деятельность сотрудников ОПК-17.У.2 уметь обеспечивать соответствие реализуемой системы требованиям Федерального законодательства, нормативно-методических документов ФСБ России, ФСТЭК России и договорным обязательствам в части ИБ ОПК-17.В.1 владеть навыками создания механизма оперативного реагирования на угрозы информационной безопасности ОПК-17.В.2 владеть обеспечения непрерывности критических бизнес-процессов
Общепрофессиональные компетенции	*ОПК-18 Способен разрабатывать и эксплуатировать системы защиты информации открытых информационных систем	ОПК-18.З.1 знать средства разработки систем защиты информации открытых информационных систем; требования нормативных документов и стандартов в области информационной безопасности ОПК-18.З.2 знать параметры эксплуатации открытых автоматизированных систем с обеспечением их информационной безопасности ОПК-18.У.1 уметь проектировать, разрабатывать, внедрять и эксплуатировать открытые автоматизированные информационные системы с реализацией подсистемы защиты информации ОПК-18.В.1 владеть навыками работы в открытых информационных системах, оценки и реализации мер защиты информации, поддержания требуемого уровня информационной безопасности
Общепрофессиональные компетенции	*ОПК-19 Способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах	ОПК-19.З.1 знать понятия конфиденциальности и целостности информации, методы верификации данных в открытых информационных системах ОПК-19.У.1 уметь осуществлять контроль и управление доступом в открытых информационных системах, управлять процессами аутентификации, идентификации пользователей и верификации данных

		ОПК-19.В.1 владеть навыками реализации систем контроля и мониторинга информационной безопасности и защиты данных в открытых информационных системах
Профессиональные компетенции	*ПК-1 Способен выполнять работы по проектированию автоматизированных информационных систем	ПК-1.З.1 знать варианты сетевой архитектуры; технологии виртуализации серверов ПК-1.З.2 знать методики обеспечения надежности и безопасности информационно-коммуникационных систем; принципы функционирования информационно-коммуникационных систем ПК-1.У.1 уметь выполнять аудит основных функциональных возможностей информационно-коммуникационной системы ПК-1.У.2 уметь выявлять ключевые требования пользователей к информационно-коммуникационным системам ПК-1.В.1 владеть навыками сбора сведений для информационно-коммуникационной системы и межсетевых соединений ПК-1.В.2 владеть навыками выбора наилучшей конфигурации информационной системы ПК-1.В.3 владеть навыками анализа данных о функционировании информационно-коммуникационных систем
Профессиональные компетенции	*ПК-2 Способен формировать требования к защите информации в открытых информационных системах	ПК-2.З.1 знать основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в вычислительных сетях ПК-2.З.2 знать программно-аппаратные средства обеспечения защиты информации автоматизированных систем ПК-2.З.3 знать способы реализации угроз безопасности в автоматизированных системах ПК-2.З.4 знать последствия от нарушения свойств безопасности информации ПК-2.З.5 знать основные угрозы безопасности информации и модели нарушителя в автоматизированных системах

		ПК-2.З.6 знать методики сертификационных испытаний технических средств защиты информации от "утечки" по техническим каналам на соответствие требованиям по безопасности информации ПК-2.З.7 знать методы защиты информации от "утечки" по техническим каналам ПК-2.У.1 уметь производить выбор программно-аппаратных средств защиты информации для использования их в составе автоматизированной системы ПК-2.У.2 уметь формировать перечень мероприятий по предотвращению угроз безопасности информации автоматизированной системы ПК-2.У.3 уметь систематизировать результаты проведенных исследований ПК-2.У.4 уметь анализировать возможные уязвимости информационных систем ПК-2.У.5 уметь выявлять известные уязвимости информационных систем ПК-2.У.6 уметь разрабатывать проекты нормативных документов, регламентирующих работу по защите информации в автоматизированных системах ПК-2.В.1 владеть навыками формирования разделов технических заданий на создание систем защиты информации автоматизированных систем, определение комплекса мер для защиты информации автоматизированных систем ПК-2.В.2 владеть навыками обоснования перечня сертифицированных средств защиты информации, необходимых для создания системы защиты информации автоматизированной системы ПК-2.В.3 владеть навыками анализа требований к назначению, структуре и конфигурации создаваемой автоматизированной системы с целью выявления угроз безопасности информации

		ПК-2.В.4 владеть навыками определения структурно-функциональных характеристик информационной системы в соответствии с требованиями нормативных правовых документов в области защиты информации.
Профессиональные компетенции	*ПК-3 Способен разрабатывать средства защиты сетей связи от несанкционированного доступа	ПК-3.З.1 знать средства анализа и контроля защищенности средств защиты средств связи сетей электросвязи ПК-3.З.2 знать угрозы безопасности, информационные воздействия, критерии оценки защищенности и методы обеспечения информационной безопасности ПК-3.У.1 уметь проводить проверку работоспособности и эффективности применяемых программно-аппаратных средств защиты информации ПК-3.У.2 уметь решать типовые задачи помехоустойчивого кодирования и декодирования сообщений ПК-3.У.3 уметь организовывать подготовку научно-технических отчетов, обзоров, публикаций по результатам выполненных исследований ПК-3.В.1 владеть навыками оценки уязвимости сетей ПК-3.В.2 владеть навыками проектирования элементов средств и систем защиты информации
Профессиональные компетенции	*ПК-4 Способен осуществлять работы по разработке систем защиты информации автоматизированных систем	ПК-4.З.1 знать способы реализации несанкционированного доступа к информации и специальных программных воздействий на информацию и ее носители в автоматизированных системах ПК-4.З.2 знать особенности защиты информации в открытых информационных системах ПК-4.З.3 знать критерии оценки эффективности и надежности средств защиты информации программного обеспечения автоматизированных систем ПК-4.З.4 знать принципы формирования политики информационной безопасности в

		автоматизированных системах ПК-4.У.1 уметь классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности ПК-4.У.2 уметь определять типы субъектов и объектов доступа, являющихся объектами защиты ПК-4.У.3 уметь выбирать меры защиты информации, подлежащие реализации в открытой автоматизированной системе ПК-4.У.4 уметь определять виды и типы средств защиты информации, обеспечивающие реализацию технических мер защиты информации ПК-4.В.1 владеть навыками разработки модели угроз безопасности информации и модели нарушителя в автоматизированных системах ПК-4.В.2 владеть навыками разработки предложений по совершенствованию системы управления безопасностью информации в открытых информационных системах
Профессиональные компетенции	*ПК-5 Способен осуществлять работы по проектированию и разработке автоматизированных систем в защищенном исполнении	ПК-5.З.1 знать технологии разработки автоматизированных систем в защищенном исполнении ПК-5.З.2 знать состав проектной документации на разработку информационных систем ПК-5.У.1 уметь строить инфологическую модель предметной области ПК-5.У.2 уметь выбирать эффективную технологию реализации защищенной автоматизированной системы на базе моделирования ПК-5.У.3 уметь разрабатывать отдельные компоненты автоматизированных систем в защищенном исполнении ПК-5.В.1 владеть принципами построения защищенных автоматизированных систем ПК-5.В.2 владеть методами проектирования автоматизированных систем в защищенном исполнении
Профессиональные компетенции	*ПК-6 Способен осуществлять управление проектами	ПК-6.З.1 знать основы теории систем и системного анализа; методики описания и моделирования бизнес-

	по созданию (модификации) автоматизированных информационных систем	процессов, средства моделирования бизнес-процессов ПК-6.З.2 знать сетевые протоколы; основы современных операционных систем ПК-6.З.3 знать основы современных систем управления базами данных ПК-6.У.1 уметь разрабатывать регламентные документы по созданию (модификации) автоматизированных информационных систем ПК-6.У.2 уметь анализировать исходную документацию по созданию (модификации) автоматизированных информационных систем ПК-6.У.3 уметь планировать работы по созданию (модификации) автоматизированных информационных систем ПК-6.В.1 владеть навыками разработки и выбора инструментов и методов описания бизнес-процессов
Профессиональные компетенции	*ПК-7 Способен управлять развитием средств защиты открытых информационных систем от несанкционированного доступа	ПК-7.З.1 знать порядок сертификации средств и систем защиты от несанкционированного доступа ПК-7.З.2 знать порядок заказа и поставки программных, программно-аппаратных и технических средств и систем защиты информации от несанкционированного доступа ПК-7.У.1 уметь проводить анализ угроз несанкционированного доступа ПК-7.У.2 уметь применять методологию менеджмента рисков информационной безопасности в открытых информационных системах ПК-7.В.1 владеть навыками организации и контроля за выполнением работ по развитию и модернизации систем защиты информации
Профессиональные компетенции	*ПК-8 Способен осуществлять эксплуатацию автоматизированных систем в защищенном исполнении	ПК-8.З.1 знать методологические основы, методы и средства построения автоматизированных систем ПК-8.З.2 знать структуру функциональной и обеспечивающей частей защищенных автоматизированных систем ПК-8.У.1 уметь решать задачи построения и эксплуатации распределенных автоматизированных

		систем обработки данных ПК-8.У.2 уметь восстанавливать работоспособность компонентов автоматизированных систем ПК-8.В.1 владеть навыками настройки автоматизированных систем для поддержки процессов организационного управления ПК-8.В.2 владеть навыками наладки и обслуживания автоматизированных систем на всех этапах жизненного цикла
Профессиональные компетенции	*ПК-9 Способен осуществлять работы по оценке работоспособности и эффективности применяемых программно-аппаратных средств защиты информации	ПК-9.З.1 знать методы и средства получения, обработки и передачи информации в операционных системах, системах управления базами данных и компьютерных сетях ПК-9.З.2 знать порядок организации работ по защите информации ПК-9.З.3 знать формальные модели управления доступом ПК-9.З.4 знать криптографические алгоритмы и особенности их программной реализации ПК-9.З.5 знать организационные меры по защите информации ПК-9.У.1 уметь использовать приемы защитного программирования, защиты от типовых атак компьютерных систем ПК-9.У.2 уметь применять методы и приемы отладки программных модулей, методы и средства тестирования ПК-9.В.1 владеть навыками разработки технических заданий, планов и графиков проведения работ, оценки технико-экономического уровня и эффективности предлагаемых решений
Профессиональные компетенции	*ПК-10 Способен осуществлять организацию работ по выполнению в автоматизированных системах требований защиты информации	ПК-10.З.1 знать источники и классификацию угроз информационной безопасности ПК-10.З.2 знать защитные механизмы и средства обеспечения безопасности автоматизированных систем ПК-10.У.1 уметь определять методы управления доступом, типы доступа и правила разграничения доступа ПК-10.У.2 уметь классифицировать защищаемую информацию по видам тайны и степени конфиденциальности

		ПК-10.В.1 владеть навыками формирования комплекса средств и мер для защиты информации в автоматизированных системах ПК-10.В.2 владеть навыками организации процесса разработки моделей угроз и моделей нарушителя безопасности компьютерных систем
Профессиональные компетенции	*ПК-11 Способен проводить оценку уровня информационной безопасности открытых информационных систем	ПК-11.З.1 знать методы и методики оценки безопасности программно-аппаратных средств защиты информации ПК-11.З.2 знать принципы построения подсистем защиты информации ПК-11.З.3 знать методы оценки эффективности политики безопасности ПК-11.У.1 уметь определять параметры функционирования средств защиты информации, разрабатывать методики оценки их защищенности, оценивать эффективность защиты информации ПК-11.У.2 уметь проводить анализ средств защиты с целью определения уровня обеспечиваемой ими защищенности и доверия ПК-11.В.1 владеть навыками оценки работоспособности применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик ПК-11.В.2 владеть навыками оценки эффективности применяемых средств защиты информации, определение их уровня защищенности
Профессиональные компетенции	*ПК-12 Способен проводить исследования в области оценки эффективности технологий автоматизации открытых информационных систем	ПК-12.З.1 знать принципы организации информационно-аналитической деятельности ПК-12.З.2 знать методы построения и исследования математических моделей в области автоматизации информационно-аналитической деятельности ПК-12.У.1 уметь решать задачи исследования информационно-аналитических систем методами моделирования ПК-12.У.2 уметь применять научные методы оценки эффективности автоматизации

		ПК-12.В.1 владеть навыками обработки, анализа и систематизации научно-технической информации в области эффективных технологий автоматизации информационно-аналитической деятельности

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
11	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»
Информатика
Основы теории информации
Дискретная математика
Техноэтика
Учебная практика
Философия
Вычислительная математика
УК-2 «Способен управлять проектом на всех этапах его жизненного цикла»
Информатика
Экономика
Основы управления проектами
УК-3 «Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели»
Социология
Техноэтика
УК-4 «Способен применять современные коммуникативные технологии, в том числе на

иностранном(ых) языке(ах), для академического и профессионального взаимодействия»
Иностранный язык
Информатика
Деловая коммуникация
Коммуникативные практики
УК-5 «Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия»
История (история России, всеобщая история)
Философия
Культурология
УК-6 «Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни»
Информатика
Социология
Техноэтика
Психология
УК-7 «Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности»
Физическая культура
Прикладная физическая культура (элективный модуль)
УК-8 «Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов»
Безопасность жизнедеятельности
УК-9 «Способен принимать обоснованные экономические решения в различных областях жизнедеятельности»
Экономика
УК-10 «Способен формировать нетерпимое отношение к коррупционному поведению»
Информационное право
Основы информационной безопасности
ОПК-1 «Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства»
Компьютерная графика
Основы информационной безопасности
Организация ЭВМ и вычислительных систем
Производственная преддипломная практика
ОПК-2 «Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности»
Компьютерная графика
Организация ЭВМ и вычислительных систем
Программно-аппаратные средства защиты информации
Основы управления проектами
Производственная преддипломная практика
ОПК-3 «Способен использовать математические методы, необходимые для решения задач профессиональной деятельности»
Математика. Аналитическая геометрия и линейная алгебра
Математика. Математический анализ

Физика
Дискретная математика
Алгоритмы и структуры данных
Теория вероятностей и математическая статистика
Электротехника
ОПК-4 «Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности»
Физика
Учебная практика
Электроника и схемотехника
Электротехника
ОПК-5 «Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации»
Основы информационной безопасности
Безопасность вычислительных сетей
Безопасность операционных систем
Безопасность систем баз данных
Организационное и правовое обеспечение информационной безопасности
Производственная преддипломная практика
ОПК-6 «Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю»
Информатика
Организационное и правовое обеспечение информационной безопасности
Производственная преддипломная практика
ОПК-7 «Способен создавать программы на языках общего назначения, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ»
Основы программирования
Технологии и методы программирования
ОПК-8 «Способен применять методы научных исследований при проведении разработок в области защиты информации в автоматизированных системах»
Производственная практика (научно-исследовательская работа)
ОПК-9 «Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации»
Информатика
Электроника и схемотехника
Организация ЭВМ и вычислительных систем
Безопасность вычислительных сетей
Безопасность операционных систем
Безопасность систем баз данных
Программно-аппаратные средства защиты информации
Сети и системы передачи информации
Разработка и эксплуатация автоматизированных систем в защищенном исполнении
ОПК-10 «Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности»

Методы и средства криптографической защиты информации
Производственная преддипломная практика
ОПК-11 «Способен разрабатывать компоненты систем защиты информации автоматизированных систем»
Защита информации от утечки по техническим каналам
Разработка и эксплуатация автоматизированных систем в защищенном исполнении
Производственная преддипломная практика
ОПК-12 «Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем»
Организация ЭВМ и вычислительных систем
Безопасность вычислительных сетей
Безопасность операционных систем
Безопасность систем баз данных
Сети и системы передачи информации
Защита информации в распределенных информационных системах
Производственная преддипломная практика
ОПК-13 «Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем»
Сети и системы передачи информации
Защита информации от утечки по техническим каналам
Управление информационной безопасностью
Производственная преддипломная практика
ОПК-14 «Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико- экономического обоснования проектных решений»
Разработка и эксплуатация автоматизированных систем в защищенном исполнении
Основы управления проектами
Производственная преддипломная практика
ОПК-15 «Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем»
Сети и системы передачи информации
Защита информации в распределенных информационных системах
Управление информационной безопасностью
ОПК-16 «Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма»
История (история России, всеобщая история)
ОПК-17 «Способен разрабатывать и реализовывать политику информационной безопасности открытых информационных систем»
Защита информации в распределенных информационных системах
Управление информационной безопасностью
Производственная преддипломная практика
ОПК-18 «Способен разрабатывать и эксплуатировать системы защиты информации открытых информационных систем»
Разработка и эксплуатация автоматизированных систем в защищенном исполнении
Производственная преддипломная практика
ОПК-19 «Способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах»

Основы информационной безопасности
Разработка и эксплуатация автоматизированных систем в защищенном исполнении
Управление информационной безопасностью
Производственная преддипломная практика
ПК-1 «Способен выполнять работы по проектированию автоматизированных информационных систем»
Открытые информационные системы
Надежность информационных систем
Нечеткая логика
Производственная практика
Теория графов и ее приложения
Защита информации в сенсорных сетях
Проектирование безопасных информационных систем
Технологии Интернета вещей
Экономическое обоснование программных проектов
Информационная безопасность распределенных информационных систем
Методы проектирования защищенных распределенных информационных систем
ПК-2 «Способен формировать требования к защите информации в открытых информационных системах»
Мультимедиа технологии
Теория кодирования
Технологии обработки аудио- и видеоданных
Постквантовая криптография
Техническая защита информации
Защита нейронных сетей
Защита от вредоносных программ
Производственная практика
Защита информации в сенсорных сетях
Научно-технический семинар
Проектирование безопасных информационных систем
Технологии Интернета вещей
Защита банковской информации
Информационная безопасность распределенных информационных систем
Методы проектирования защищенных распределенных информационных систем
Технологии защиты электронных платежей
Технология построения защищенных распределенных приложений
ПК-3 «Способен разрабатывать средства защиты сетей связи от несанкционированного доступа»
Основы радиотехники
Теория систем и системный анализ
Микропроцессорная техника
Теория кодирования
Устройства и системы беспроводной связи
Моделирование систем
Постквантовая криптография
Надежность информационных систем
Научно-технический семинар
Проектирование безопасных информационных систем
Экономическое обоснование программных проектов
Информационная безопасность распределенных информационных систем
Методы проектирования защищенных распределенных информационных систем

Технология построения защищенных распределенных приложений
ПК-4 «Способен осуществлять работы по разработке систем защиты информации автоматизированных систем»
Методы и средства проектирования информационных систем
Надежность информационных систем
Нечеткая логика
Теория графов и ее приложения
Проектирование безопасных информационных систем
Экономическое обоснование программных проектов
Защита банковской информации
Информационная безопасность распределенных информационных систем
Методы проектирования защищенных распределенных информационных систем
Технологии защиты электронных платежей
Технология построения защищенных распределенных приложений
ПК-5 «Способен осуществлять работы по проектированию и разработке автоматизированных систем в защищенном исполнении»
Теория систем и системный анализ
Микропроцессорная техника
Мультимедиа технологии
Технологии обработки аудио- и видеоданных
Интеллектуальные системы и технологии
Моделирование систем
Исследование операций и теории игр
Методы и средства проектирования информационных систем
Производственная практика
Предметно-ориентированные автоматизированные информационные системы
Проектирование безопасных информационных систем
Экономическое обоснование программных проектов
Методы проектирования защищенных распределенных информационных систем
Разработка мобильных приложений
Технология построения защищенных распределенных приложений
ПК-6 «Способен осуществлять управление проектами по созданию (модификации) автоматизированных информационных систем»
Теория систем и системный анализ
Открытые информационные системы
Моделирование систем
Методы и средства проектирования информационных систем
Защита информации в сенсорных сетях
Проектирование безопасных информационных систем
Технологии Интернета вещей
ПК-7 «Способен управлять развитием средств защиты открытых информационных систем от несанкционированного доступа»
Стандарты информационной безопасности
Техническая защита информации
Научно-технический семинар
Проектирование безопасных информационных систем
Защита банковской информации
Информационная безопасность распределенных информационных систем
Технологии защиты электронных платежей
ПК-8 «Способен осуществлять эксплуатацию автоматизированных систем в защищенном исполнении»

Микропроцессорная техника
Устройства и системы беспроводной связи
Открытые информационные системы
Производственная практика
Исследование операций и теории игр
Методы и средства проектирования информационных систем
Научно-технический семинар
Проектирование безопасных информационных систем
Методы проектирования защищенных распределенных информационных систем
ПК-9 «Способен осуществлять работы по оценке работоспособности и эффективности применяемых программно-аппаратных средств защиты информации»
Стандарты информационной безопасности
Математические основы обработки информации
Мультимедиа технологии
Технологии обработки аудио- и видеоданных
Устройства и системы беспроводной связи
Производственная практика
Интеллектуальные системы и технологии
Постквантовая криптография
Защита нейронных сетей
Защита от вредоносных программ
Методы и средства проектирования информационных систем
Защита информации в сенсорных сетях
Научно-технический семинар
Технологии Интернета вещей
Экономическое обоснование программных проектов
Защита банковской информации
Информационная безопасность распределенных информационных систем
Распознавание образов
Технологии защиты электронных платежей
Технология построения защищенных распределенных приложений
ПК-10 «Способен осуществлять организацию работ по выполнению в автоматизированных системах требований защиты информации»
Стандарты информационной безопасности
Производственная практика
Техническая защита информации
Проектирование безопасных информационных систем
Информационная безопасность распределенных информационных систем
Методы проектирования защищенных распределенных информационных систем
Распознавание образов
ПК-11 «Способен проводить оценку уровня информационной безопасности открытых информационных систем»
Открытые информационные системы
Производственная практика
Защита нейронных сетей
Защита от вредоносных программ
Защита информации в сенсорных сетях
Научно-технический семинар
Предметно-ориентированные автоматизированные информационные системы
Проектирование безопасных информационных систем
Технологии Интернета вещей

Экономическое обоснование программных проектов
Защита банковской информации
Информационная безопасность распределенных информационных систем
Методы проектирования защищенных распределенных информационных систем
Технологии защиты электронных платежей
Технология построения защищенных распределенных приложений
ПК-12 «Способен проводить исследования в области оценки эффективности технологий автоматизации открытых информационных систем»
Вычислительная математика
Учебная практика
Математические основы обработки информации
Мультимедиа технологии
Теория информационной безопасности и методы защиты информации
Технологии обработки аудио- и видеоданных
Моделирование систем
Исследование операций и теории игр
Надежность информационных систем
Нечеткая логика
Теория графов и ее приложения
Научно-технический семинар
Распознавание образов

4.1.3. Методические рекомендации обучающимся по подготовке к ГЭ.

Методические рекомендации Государственный экзамен является составной частью ГИА и представляет собой форму оценки знаний, навыков самостоятельной работы, и способности применять их для решения практических задач, полученных обучающимся в процессе освоения ОП за весь период обучения.

ГЭ проводится по нескольким дисциплинам ОП, результаты освоения которых имеют определяющее значение для профессиональной деятельности выпускников. ГЭ проводится в письменной форме и завершается аттестационной оценкой «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Оценки «отлично», «хорошо», «удовлетворительно» означают успешное прохождение государственного аттестационного испытания. На экзамен выделяется четыре академических часа.

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 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.

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

Экзаменационные билеты для проведения ГЭ формируются согласно списку вопросов для ГЭ, каждый билет включает четыре вопроса.

Вопросы к государственному экзамену подразделяются на 4 блока, включающих вопросы из различных разделов четырех основополагающих дисциплин учебного плана.

Блок 1 Проектирование информационных систем (ИС)

Тема 1.1 Модели жизненного цикла ИС

Тема 1.2 Архитектуры ИС

Тема 1.3 Базы данных

Тема 1.4 Методы и средства проектирования информационных систем

Тема 1.5 Методологии системного и объектно-ориентированного анализа предметной области

Блок 2 Методы и технологии программирования

Тема 2.1 Методология объектно-ориентированного программирования

Тема 2.2 Технологические средства разработки программного обеспечения

Тема 2.3 Методы отладки и тестирования программ

Тема 2.4 Технологии коллективной разработки программного обеспечения

Тема 2.5 Языки программирования

Блок 3 Криптографическая защита информации

Тема 3.1 Принципы построения криптографических алгоритмов и протоколов

Тема 3.3 Типы криптографических алгоритмов и протоколов

Тема 3.4 Модели и характеристики криптографических алгоритмов и протоколов

Тема 3.5 Криптоанализ и методы оценки криптостойкости

Блок 4 Управление информационной безопасностью

Тема 4.1 Стандартизация в области управления информационной безопасностью

Тема 4.2 Процессный подход к управлению информационной безопасностью

Тема 4.3 Политика безопасности предприятия

Тема 4.4 Модели угроз информационной безопасности

Тема 4.5 Модели защиты и профили защиты

Тема 4.6 Методы выявления уязвимостей и оценки рисков

Тема 4.7 Системы управления информационной безопасностью. SIEM-системы

Основными критериями оценки уровня подготовки и сформированности соответствующих компетенций выпускника при проведении государственного экзамена в письменной форме являются:

- степень владения профессиональной терминологией;
- уровень усвоения студентом теоретических знаний и умение использовать их для решения профессиональных задач;
- ориентирование в нормативных правовых актах, научной и иной специальной литературе;
- логичность, обоснованность, четкость ответа;
- культура ответа.

Оценка «отлично» выставляется при условии выполнения следующих требований:

1) Выпускник демонстрирует:
- свободное владение профессиональной терминологией;
- высокий уровень теоретических знаний и умение использовать их для решения профессиональных задач;
- исчерпывающее последовательное, обоснованное и логически стройное изложение ответа, без ошибок;
- демонстрируют знание современной учебной и научной литературы;
- демонстрирует глубокие знания базовых нормативно-правовых актов;
- демонстрируют способность к анализу и сопоставлению различных подходов к решению заявленной в билете проблематики.

2) Выпускник без затруднений ориентируется в нормативных правовых актах, научной и иной специальной литературе.

3) Письменная речь выпускника грамотная, лаконичная, с правильной расстановкой акцентов.

Оценка «хорошо» выставляется при условии выполнения следующих требований:

1) Выпускник демонстрирует:
- владение профессиональной терминологией на достаточном уровне;
- достаточный уровень теоретических знаний и умение использовать их для решения профессиональных задач;
- грамотное и логичное изложение ответа, без существенных ошибок, но изложение недостаточно систематизировано и последовательно.

2) Выпускник с некоторыми затруднениями ориентируется в нормативных правовых актах, научной и иной специальной литературе.
3) Письменная речь выпускника грамотная, лаконичная, с правильной расстановкой акцентов.

Оценка «удовлетворительно» выставляется при условии выполнения следующих требований:

1) Выпускник демонстрирует:
- владение профессиональной терминологией на минимальном уровне;
- низкий пороговый уровень теоретических знаний, усвоил только основной программный материал без знания отдельных особенностей;
- при ответе допускает неточности, материал недостаточно систематизирован;
- нарушения в последовательности изложения.

2) Выпускник с затруднениями ориентируется в нормативных правовых актах, научной и иной специальной литературе.
3) Письменная речь выпускника в основном грамотная, но не демонстрируется уверенное владение материалом.

Оценка «неудовлетворительно» выставляется при условии:

1) Выпускник не владеет профессиональной терминологией, демонстрирует низкий уровень теоретических знаний и умения использовать их для решения профессиональных задач.
2) Выпускник не знает значительной части программного материала, допускает существенные грубые ошибки, не ориентируется в нормативных правовых актах, научной и иной специальной литературе.
3) Письменная речь недостаточно грамотная. Критическое количество ошибок допущено обучающимся по подготовке к ГЭ.

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.

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 специальности 10.05.03, дипломные работы студентов должны отражать один или несколько видов 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)

Работа студента над ВКР по специальности 10.05.03 может вестись в двух направлениях, определяющих состав и структуру основной части работы: проектное и научно-исследовательское. ВКР в виде проекта имеет своей основной целью достижение практической значимости для конкретного объекта: предприятия, подразделения, рабочего места, группы людей, общества и.т.д. Как правило, такая работа имеет хорошо выраженный экономический, социальный, экологический и др. эффект. Научная работа имеет своей целью разработку методов, моделей и методик для некоторых видов объектов и субъектов предметной области. Как правило, такая работа имеет поставленную гипотезу, построенную модель, проведенный эксперимент и обоснованные выводы. Объем основной части работы должен составлять 50-80 листов. Весь объем основной части рекомендуется разделить на 3-4 главы.

Для специальности 10.05.03 «Информационная безопасность автоматизированных систем» предлагается следующая структура основной части ВКРС практической направленности:

1) описание предприятия, организационная структура, описание рабочих мест;

2) системный (структурный или объектно-ориентированный) анализ предметной области, построение диаграмм IDEF0 as-is, DFD as-is, UML-диаграмм и др., функционально-стоимостной и функционально-временной анализ;
3) реинжиниринг бизнес-процессов, построение диаграмм IDEF0 to-be, DFD to-be, UML-диаграмм и др., функционально-стоимостной и функционально-временной анализ;
4) инфологическое моделирование, построение диаграмм ER и/или ORM стратегического и логического уровней;
5) архитектура проектируемой информационной системы;
6) выбор и обоснование средств реализации построенных моделей.
7) разработка серверных и клиентской частей программного приложения:
8) решение проблем информационной безопасности и защиты информации: организационные, технические, программные вопросы защиты информации;
9) экономическое обоснование проекта и/или оценка рисков.

Предлагается следующая структура основной части ВКР научной направленности:

1) **актуальность темы** работы может быть представлена как:
- социально-политическая актуальность – обоснование необходимости разрабатывать данную тему с точки зрения современной общественно-политической ситуации, накопившихся социальных проблем;
- научная актуальность – сложившаяся внутри науки ситуация необходимости именно сейчас разработать именно эту тему. Теоретический аспект – недостаточная разработка данного вопроса в теории. Практический аспект – неэффективная работа в данном направлении на современном этапе;

2) **объект, предмет исследования**. Объект исследования - это явление или процесс объективной реальности, на который направлен научный поиск автора работы. Объект выделяется на основании анализа избранной исследователем проблемы, перечень объектов профессиональной деятельности для специальностей 10.05.03 и 10.05.05 приведен ниже. Предмет исследования – это фрагмент объекта, какая-то его сторона, например, уязвимости, атаки, передача и хранение информации, риски ИБ и др. Предмет устанавливает познавательные границы исследования. Один и тот же объект может предполагать множество предметов исследования. Предмет исследования чаще всего либо совпадает с его темой, либо они очень близки по звучанию;
3) **цель и задачи исследования.** Цель – стратегия исследования, его границы. То, что должно быть достигнуто в итоге работы. Задачи – тактика исследования; путь достижения цели, последовательные шаги продвижения к цели. Цель формулируется глаголом в неопределенной форме (изучить, описать, установить, выяснить, рассмотреть, проанализировать и т.д.), либо существительным в именительном падеже (изучение, анализ, выявление и т.д.). Задачи формулируются глаголами в неопределенной форме;
4) **гипотеза.** Гипотеза – это предположение, истинность которого еще не доказана, прогноз. В ходе проведения исследования гипотеза может быть подтверждена, уточнена, опровержена. Это обязательно указывается в заключении;
5) **обзор и анализ литературных источников** по теме исследования. Целесообразно рассмотреть, в каком состоянии на современном этапе находится избранное научное направление, что уже сделано другими авторами, что в этом вопросе еще неясно и поэтому требует дальнейшего исследования;
6) **методы исследования.** Описываются методики исследования и контингент испытуемых. Достаточно подробно следует изложить организацию эксперимента, описать методики, дать подробные сведения об испытуемых. Прочитав эту главу, не должно возникать вопросов о том, как получены те или иные данные и

результаты. Любой прочитавший ее должен понять, как провести аналогичное исследование;

7) **результаты исследования**. Обычно приводится изложение собственных результатов исследования. В ней часто размещают таблицы с полученными данными (не первоначальными, а уже обработанными), рисунки, обобщающие или иллюстрирующие результаты, пояснения автора по поводу тех или иных полученных данных. Обычно, эта глава разбивается на параграфы, в соответствии с логикой изложения материала;
8) **выводы и практические рекомендации.** Количество выводов должно соответствовать количеству поставленных задач (и в идеале – представлять собой решение этих задач). Однако, на практике такое встречается редко. Одной задаче может соответствовать два вывода, реже - выводы мало соответствуют поставленным задачам. Несоответствия выводов поставленным задачам следует избегать. Также приводятся практические рекомендации, формулирующиеся исходя из данных эксперимента:

- автоматизированные системы, функционирующие в условиях существования угроз в информационной сфере и обладающие информационно-технологическими ресурсами, подлежащими защите;
- информационные технологии, формирующие информационную инфраструктуру в условиях существования угроз в информационной сфере и задействующие информационно-технологические ресурсы, подлежащие защите;
- технологии обеспечения информационной безопасности автомптизированных систем;
- системы управления информационной безопасностью автоматизированных систем.

Объектами профессиональной деятельности выпускников по специальности 10.05.03 являются:

- объекты информатизации, включая компьютерные, автоматизированные, телекоммуникационные, информационные и информационно-аналитические системы, информационные ресурсы и информационные технологии в условиях существования угроз в информационной сфере;
- технологии обеспечения информационной безопасности объектов различного уровня (система, объект системы, компонент объекта), которые связаны с информационными технологиями, используемыми на этих объектах;

процессы управления информационной безопасностью защищаемых объектов.

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).

Необходимо соблюдать следующие требования к содержанию списка литературы:

Требование 1. Дипломная работа должна быть написана на основе 30 и более источников.

Требование 2. Используемая литература должна быть актуальной (желательно не старше 5 лет). Количество книг и документов 10-20-летней давности не должно превышать 30% от общего объема.

Материалы старше 20 лет использовать запрещается. Однако из этого правила есть исключения – такие материалы можно приводить в качестве источника, если научная работа предполагает историческую справку или исследование архивов.

Требование 3. Электронные источники должны составлять не более половины от общего количества источников.

Требование 4. Каждый источник, указанный в списке литературы, должен быть использован в тексте работы.

Требование 5. Каждый источник (вне зависимости от вида) достаточно упомянуть в списке литературы один раз. При этом не важно, сколько раз информация из него используется в тексте работы.

Требование 6. Все используемые материалы должны обязательно соответствовать тематике работы.

Требование 7. Не менее 10% источников должны быть на иностранном языке.

Важно! При проверке работы на процент заимствований и плагиата список литературы не учитывается, равно как и цитаты.

Правильно оформленный список литературы показывает качество написания ВКР. Составлять его лучше в процессе написания – при упоминании какого-либо источника лучше сразу вносить его в список. Каждая ссылка в тексте должна вести на соответствующий источник в списке использованных источников.

Приложения

Приложения к дипломной работе по специальностям 10.05.03 и 10.05.05 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 10.05.03 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 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 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.

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.

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.

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 (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.).

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_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.

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 практикум / С. В. Беззатеев, С. Г. Фомичева ; С.-Петерб. 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.-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.	5

	Бакай ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - Санкт-Петербург : Изд-во ГУАП, 2020. - 133 с.	
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

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 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. 52-48

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 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 форме

№ п/п	Список вопросов для ГЭ, проводимого в письменной форме	Компетенции
1	Модели системного анализа предметной области	*УК-1 Способен

	IDEF0, DFD, ER. Процесс принятия решений в области обеспечения информационной безопасности автоматизированных систем. Инфологическое моделирование. Цели, задачи, методы.	осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий
2	Проектная и операционная деятельность. Функциональное и проектное управление Жизненный цикл проекта создания системы информационной безопасности объекта защиты. Анализ угроз и методы снижения рисков при проектировании АИС Основные принципы управления ресурсами проекта.	*УК-2 Способен управлять проектом на всех этапах его жизненного цикла
3	Психологические аспекты управления проектной командой Формирование и развитие команды проекта. Организация эффективной деятельности команды	*УК-3 Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели
4	Понятие «современная коммуникация»: сущность и характеристика. Особенности современной коммуникации Стандартные стеки коммуникационных протоколов	*УК-4 Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия
5	Методы оценки субъективного фактора в процессе принятия решений Карьерные траектории и жизненные стратегии в области информационной безопасности и защиты информации	*УК-6 Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни
6	Требования, предъявляемые к гражданам, поступающим на службу в органы федеральной службы безопасности	*УК-7 Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной

		деятельности
7	Требования к организации рабочего места специалиста по информационной безопасности автоматизированных информационных систем	*УК-8 Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов
8	Методы и модели оценки экономической эффективности проекта по разработке и внедрению системы информационной безопасности Экономический подход к оценке эффективности комплексных систем защиты информации	*УК-9 Способен принимать обоснованные экономические решения в различных областях жизнедеятельности
9	Особенности профилактики коррупционных преступлений, совершаемых в правоохранительных органах	*УК-10 Способен формировать нетерпимое отношение к коррупционному поведению
10	Понятие информации и информационного процесса. Роль информации в современном обществе. Необходимость защиты информации	*ОПК-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства
11	Классификация информационных технологий. Виды системного и прикладного программного обеспечения. Отечественные SIEM-системы. Особенности настройки и применения.	*ОПК-2 Способен применять программные средства системного и прикладного назначений, в том

		числе отечественного производства, для решения задач профессиональной деятельности
12	Математическая модель шифра. Математические основы обработки информации в задачах информационной безопасности. Модулярная арифметика. Кольца вычетов.	*ОПК-3 Способен использовать математические методы, необходимые для решения задач профессиональной деятельности
13	Технические каналы утечки информации, их классификация.	*ОПК-4 Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности
14	Требования к документированию государственного стандарта ЕСПД. Необходимый набор документов. Этапы разработки программного обеспечения. Постановка задачи и спецификация программы. Анализ требований, предъявляемых к программе. ГОСТ ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения	*ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации
15	Главные регуляторы в области сертификации средств защиты информации в России – ФСТЭК и ФСБ. База данных угроз ФСТЭК. Требования, предъявляемые к комплексным системам защиты информации Состав, объекты и степень конфиденциальности защищаемой информации Факторы, создающие угрозу информационной безопасности Угрозы безопасности информации	*ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности

		Российской Федерации, Федеральной службы по техническому и экспортному контролю
16	Обзор современных языков программирования. Выбор языка. Общие требования к организации программы. Выбор имен. Комментарии. Форматирование программы. Организация ввода-вывода Оптимизация программы. Стиль записи программы, форматирование и программы-форматеры. Конструирование вложенных условных операторов. Использование процедур и функций при разработке программ. Применение рекурсии. Область применения ООП. Определение объектов. Область действия полей объекта и параметр SELF. Наследование. Присваивание объектов. Полиморфизм. Динамические объекты. Записи. Файлы. Динамическик типы данных Списки. Программирование рекурсивных алгоритмов. Способы конструирования программ. Модульные программы Определение операций над типами, определяемыми пользователем. Слабая. и сильная типизация языков программирования Указатели и динамические структуры данных. Списки. Абстрактные структуры данных. Использование ссылок и надежность программ.	*ОПК-7 Способен создавать программы на языках общего назначения, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ
17	Методологические основы организации комплексных систем защиты информации Требования к технологиям проектирования, разработки и сопровождения информационных систем. Критерии оценки ресурсов проекта: информационных технологий, средств технической защиты информации, сетей и систем передачи информации.	*ОПК-9 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации
18	Классификация шифров замены. Шифр Цезаря. Шифр простой замены. Шифр Плейфера. Полибианский квадрат. Шифр Хилла. Шифр Виженера. Частотный анализ. Тест Казиски. Основные понятия и определения криптографии. Виды криптосистем. Задачи, решаемые методами криптографии. Виды информации, подлежащие закрытию, их модели и свойства. Частотные характеристики открытых сообщений. Критерии на открытый текст. Особенности нетекстовых сообщений.	*ОПК-10 Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности

	Классификация шифров перестановки. Примеры шифров перестановки и их криптоанализ. Шифры гаммирования. Шифр Вернама. Подходы к его криптоанализу. Композиции шифров. Enigma. Шифр Хейглина. Математическая модель шифра. Атаки и угрозы шифрам.	
19	Особенности помещений как объектов защиты для работы по защите информации Особенности синтеза СЗИ АС от НСД Методика синтеза СЗИ Оптимальное построение системы защиты для АС Проектирование системы зашиты информации для существующей АС	*ОПК-11 Способен разрабатывать компоненты систем защиты информации автоматизированных систем
20	Иерархическая и сетевая модели данных Элементы реляционной модели данных Реляционное исчисление. Организация процессов обработки данных в БД. Ограничения целостности Жизненный цикл БД. Модели жизненного цикла ПО Принципы построения БД. Нормальные формы Транзакции. Сериализация транзакций. Принципы построения БД. Метод «Сущность-связь	*ОПК-12 Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем
21	Этап тестирование информационной системы. План тестирования. Основы доказательства правильности. Тестирование и отладка. Различие между отладкой и тестированием. Выбор алгоритма.	*ОПК-13 Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем
22	Задачи и функции информационных систем Технологии проектирования информационных систем Основные модели жизненного цикла информационных систем Общая характеристика процесса проектирования информационных систем Технико- экономическое обоснование проектных решений	*ОПК-14 Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений
23	Основные направления государственной политики в сфере информатизации. Нормативные документы	*ОПК-16 Способен анализировать

		основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма
24	Цели, задачи и принципы построения комплексных систем защиты информации Методологические основы организации комплексных систем защиты информации Разработка политики информационной безопасности предприятия	*ОПК-17 Способен разрабатывать и реализовывать политику информационной безопасности открытых информационных систем
25	Общая характеристика задач моделирования КСЗИ Формальные модели безопасности и их анализ. Прикладные модели защиты информации в АС. Показатель уровня защищенности, основанный на экспертных оценках.	*ОПК-18 Способен разрабатывать и эксплуатировать системы защиты информации открытых информационных систем
26	Модели нарушителей безопасности АС. Методика выявления нарушителей, тактики их действий и состава интересующей их информации Обеспечение безопасности информации в непредвиденных ситуациях.	*ОПК-19 Способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах
27	Понятие инженерии программирования. Вопросы и задачи инженерии программирования Состав и структура информационных систем, основные элементы, порядок функционирования Современные технологии проектирования информационных систем	*ПК-1 Способен выполнять работы по проектированию автоматизированных информационных систем
28	Модель угроз и оценки рисков информационной безопасности автоматизированных систем Прикладные модели защиты информации в автоматизированных системах	*ПК-2 Способен формировать требования к защите информации в открытых информационных системах
29	Модели нарушителей безопасности автоматизированных систем	*ПК-4 Способен осуществлять работы

	Особенности синтеза средств защиты информации автоматизированных систем от несанкционированного доступа	по разработке систем защиты информации автоматизированных систем
30	Цели и задачи защиты информации в автоматизированных системах Факторы, определяющие необходимость защиты периметра и здания предприятия. Состав обеспечивающих подсистем информационных систем Состав и характеристики функциональных подсистем информационных систем	*ПК-5 Способен осуществлять работы по проектированию и разработке автоматизированных систем в защищенном исполнении
31	Реинжиниринг бизнес-процессов Понятие проектирования информационных систем. Состав проекта Проектирование системы зашиты информации для существующей автоматизированной системы	*ПК-6 Способен осуществлять управление проектами по созданию (модификации) автоматизированных информационных систем
32	Оценка эффективности технических средств защиты информации Методы проведения экспертного опроса Оценка уровня надежности и безопасности автоматизированной системы.	*ПК-9 Способен осуществлять работы по оценке работоспособности и эффективности применяемых программно-аппаратных средств защиты информации
33	Требования, предъявляемые к комплексным системам защиты информации Оценка угроз безопасности информации в автоматизированных системах.	*ПК-11 Способен проводить оценку уровня информационной безопасности открытых информационных систем

Таблица 10 – Перечень задач для ГЭ, проводимого в письменной 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	ОПК-10

	переданного слова получен набор букв ЭАВЬЩО. Найдите переданное слово. Задача 2. При шифровании открытый текст разбивается 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 A и B. Из-за помех сигнала A в трех случаях из 4-х воспринимается как сигнал A и как B. Определить количество информации о воспринятом сигнале, содержащееся в поступившем сигнале, если поступления сигналов A и B на вход приемника одинаково вероятны. **2** По каналу связи передается 2 сигнала A1 и A2 с вероятностями P(A1) = P(A2) = 0.5. На выходе канала сигналы преобразуются в символы a1 и a2, причем из-за помех, которым одинаково подвержены сигналы A1 и A2, в передачу вносятся ошибки, так что в среднем один символ из 100 принимается неверно (a1 вместо a2 или a2 вместо a1). Определить среднее количество информации на символ, передаваемой по такому каналу. Сравните ее с количеством информации при отсутствии помех. **4** Имеется источник информации с производительность H = 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.	ОПК-3

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.

Оценка компетенции 5-балльная шкала	Характеристика сформированных компетенций
«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 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

Оценка компетенции 5-балльная шкала	Характеристика сформированных компетенций
	членами ГЭК вопросы; – студент неточно 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 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 70 %.

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

Проектирование блокчейн системы для реализации "отменяемой биометрии"
Проектирование системы защиты веб-сервиса для сопровождения процесса приема абитуриентов
Анализ вредоносности файлов методами бинарной классификации на основе машины опорных векторов
Разработка информационной системы учета табельного оружия в подразделениях УМВД РФ
Проектирование автоматизированной системы безопасного информационного сопровождения подготовки гоночных мероприятий на автодроме
Проектирование безопасной информационной системы по сопровождению подготовки турниров по киберспорту
Проектирование аналитической системы динамического профилирования
Проектирование защищенной информационной системы учета музейных предметов
Проектирование информационно-аналитической системы стеганоанализа растровых изображений
Проектирование аналитической системы учета технических средств отделов воинских частей РФ
Разработка аналитической информационной системы учёта межсетевых экранов в цифровых подразделениях организаций
Проектирование безопасной информационной системы сопровождения студенческих проектов
Проектирование защищенной информационной системы учета абонементов фитнес клуба
Разработка аналитической системы скрытых каналов по памяти при взаимодействии с "ГосСОПКА"
Проектирование защищенной системы учёта инструктажей по охране труда

Приложение № 2
Рецензия на программу государственной итоговой аттестации по специальности 10.05.03 «Информационная безопасность автоматизированных систем» от работодателя

ПОЛИКОМ про

РЕЦЕНЗИЯ
на программу государственной итоговой аттестации
по программе специалитета 10.05.03
«Информационная безопасность автоматизированных систем»
специализация «Безопасность открытых информационных систем»

Представленная для рецензирования рукопись Программы государственной итоговой аттестации по программе высшего образования по специальности 10.05.03 «Информационная безопасность автоматизированных систем», специализации «Безопасность открытых информационных систем», подготовленная профессорско-преподавательским составом кафедры №34 «Технологий защиты информации» Санкт-Петербургского государственного университета аэрокосмического приборостроения в соответствии с требованиями государственного образовательного стандарта высшего образования по специальности 10.05.03 «Информационная безопасность автоматизированных систем» (зарегистрирован Минюстом России 17 февраля 2021 г., регистрационный № 62532), а также государственными нормативными актами и локальными актами ГУАП.

Программа соответствует нормативным и методическим требованиям, предъявляемым к программам государственной итоговой аттестации (ГИА).

Программа состоит из общих положений, включающих цели и задачи ГИА, формы ее проведения, объемы и продолжительность. Программа ГИА включает в себя программу государственного экзамена (ГЭ) и методические рекомендации обучающимся по подготовке к ГЭ, а также требования к выпускным квалификационным работам специалиста (ВКРС) – дипломным работам (ДР) и порядку их выполнения.

ООО «Поликом Про»
195197, Российская Федерация,
г. Санкт-Петербург,
Полюстровский пр-кт, д. 59, литер Э

ОГРН: 1147847343313
ИНН: 7804541940
КПП: 780401001

р/с 40702810803000090391
в ПАО БАНК «СИАБ» г. Санкт-Петерб
к/с 30101810600000000757
БИК 044030757

ПОЛИКОМ про

Разработанная программа в полной мере обеспечивает возможность проверки и оценки приобретенных студентами теоретических знаний, практических навыков и умений по основной образовательной программе высшего образования по специальности 10.05.03 «Информационная безопасность автоматизированных систем».

Содержание программы ГИА позволяет проверить и оценить как уровень теоретической подготовки обучающихся, так и наличие у них практических навыков, необходимых для успешного осуществления профессиональной деятельности с учетов специализации образовательной программы.

Особое внимание уделено оценке уровня достижения компетенций выпускников, связанных с осознанием социальной значимости будущей профессии, профессиональными навыками в области информационной безопасности, общепрофессиональными навыками, в том числе, владением современными цифровыми технологиями.

Программа государственной итоговой аттестации по программе высшего образования по специальности 10.05.03 «Информационная безопасность автоматизированных систем», специализации «Безопасность открытых информационных систем», подготовленная профессорско-преподавательским составом кафедры №34 «Технологий защиты информации» Санкт-Петербургского государственного университета аэрокосмического приборостроения может быть рекомендована для использования при проведении государственной итоговой аттестации выпускников.

Руководитель отдела
информационной безопасности

должность	подпись, дата	А.А. Зенков
		инициалы,фамилия

М.П.

ООО «Поликом Про»
195197, Российская Федерация,
г. Санкт-Петербург,
Полюстровский пр-кт, д. 59, литер Э

ОГРН: 1147847343313
ИНН: 7804541940
КПП: 780401001

р/с 40702810803000090391
в ПАО БАНК «СИАБ» г. Санкт-Петербург
к/с 30101810600000000757
БИК 044030757

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