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

Кафедра № 33

УТВЕРЖДАЮ
Проректор по учебной деятельности
В. А. Матьяш
(подпись, фамилия)
(подпись)
«26» мая 2022 г

ПРОГРАММА ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

Код направления подготовки/ специальности	10.05.05
Наименование направления подготовки/ специальности	Безопасность информационных технологий в правоохранительной сфере
Наименование направленности	Организация и технологии защиты информации (в информационных системах)
Форма обучения	очная

Санкт-Петербург –2022

Лист согласования программы

Программу составил (а)
доц.,к.э.н.,доц. 26.05.22 Т.Н. Елина
(должность, уч. степень, звание) (подпись, дата) (инициалы, фамилия)

Программа одобрена на заседании кафедры № 33
«27» мая 2021 г, протокол № 10

Заведующий кафедрой № 33
д.т.н.,доц. 26.05.22 С.В. Безяев
(уч. степень, звание) (подпись, дата) (инициалы, фамилия)

Руководитель направления 10.05.05
проф.,д.т.н.,доц. 26.05.22 С.В. Безяев
(должность, уч. степень, звание) (подпись, дата) (инициалы, фамилия)

Ответственный за ОП ВО 10.05.05(05)
доц.,к.т.н.,доц. 26.05.22 В.А. Мышенков
(должность, уч. степень, звание) (подпись, дата) (инициалы, фамилия)

Заместитель директора института №3 по методической работе
26.05.22 Н.В. Решетникова
(должность, уч. степень, звание) (подпись, дата) (инициалы, фамилия)

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

Кафедра № 33

УТВЕРЖДАЮ
Проректор по учебной деятельности
В. А. Мальцев
(подпись)
«26» мая 2022 г

ПРОГРАММА ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

Код направления подготовки/ специальности	10.03.05
Наименование направления подготовки/ специальности	Безопасность информационных технологий в правоохранительной сфере
Наименование направленности	Организация и технология защиты информации (в информационных системах)
Форма обучения	очная

Санкт-Петербург – 2022

Лист согласования программы

Программу составил (а)
доц., д. т. н., доц. (должность, уч. степень, звание) — 26.05.22 (подпись, дата) — Т.Н. Елина (инициалы, фамилия)

Программа одобрена на заседании кафедры № 33
«27» мая 2022 г. протокол № 10

Заведующий кафедрой № 33
д. т. н., доц. (уч. степень, звание) — 26.05.22 (подпись, дата) — С.В. Беззатеев (инициалы, фамилия)

Руководитель направления 10.03.05
проф., д. т. н., доц. (должность, уч. степень, звание) — 26.05.22 (подпись, дата) — С.В. Беззатеев (инициалы, фамилия)

Ответственный за ОП ВО 10.03.05(03)
доц., д. т. н., доц. (должность, уч. степень, звание) — 26.05.22 (подпись, дата) — В.А. Мальчиков (инициалы, фамилия)

Заместитель директора института №3 по методической работе
(должность, уч. степень, звание) — 26.05.22 (подпись, дата) — Н.В. Решетникова (инициалы, фамилия)

1. ЦЕЛИ, ЗАДАЧИ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

1.1. Целью ГИА обучающихся по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере», направленности «Организация и технологии защиты информации (в информационных системах)», является установление уровня подготовки обучающихся к выполнению профессиональных задач и соответствия его подготовки, требуемой по ОП квалификации: специалист.

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 должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной	УК-7.З.1 знать виды физических упражнений; роль и значение 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 физиче-ской культуры и спорта

	деятельности	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 природопользо-вания 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 на основе анализа основных этапов и закономерностей исторического развития Российского государства, его места и роли в контексте всеобщей истории формировать устойчивые внутренние мотивы профессионально-служебной деятельности, базирующиеся на гражданской позиции, патриотизме, ответственном отношении к выполнению профессионального долга	ОПК-1.З.1 знать основные закономерности, проблемы и перспективы развития государственно-правового воздействия на общество ОПК-1.З.2 знать структуру и содержание социальных ценностей, отражаемых в праве, роль правосознания, правового мышления, правовой культуры и развития правовой системы современной России ОПК-1.З.3 знать содержание основных положений действующего информационного законодательства в сфере защиты государственной тайны ОПК-1.У.1 уметь анализировать и оценивать объем и содержание основных категорий и других понятий права ОПК-1.У.2 уметь использовать правовую методологию для развития правосознания, правового мышления и правовой культуры в сфере профессиональной деятельности ОПК-1.У.3 уметь соблюдать в профессиональной деятельности требования правовых актов в области защиты государственной тайны и информационной безопасности ОПК-1.В.1 владеть навыками правового обеспечения соблюдения режима секретности ОПК-1.В.2 владеть навыками применения норм права в профессиональной деятельности ОПК-1.В.3 владеть навыками анализа и толкования нормативных правовых актов с учетом специфики соответствующего законодательства
Общепрофессиональные компетенции	*ОПК-2 Способен анализировать мировоззренческие, социальные и личностно-значимые проблемы в целях формирования ценностных, этических основ профессионально-служебной	ОПК-2.З.1 знать принципы гуманности в контексте выполнения профессиональных обязанностей и взаимоотношений в профессиональной среде трудового коллектива при решении социальных и профессиональных задач ОПК-2.З.2 знать психологические технологии, позволяющие решать типовые задачи в области профессиональной деятельности ОПК-2.У.1 уметь осознавать

	деятельности	нравственный смысл профессиональной деятельности в рамках законности и в соответствие с требованиями Конституции РФ, этики и морали ОПК-2.У.2 уметь формулировать и отстаивать личные убеждения, свою гражданскую позицию ОПК-2.У.3 уметь применять различные психологические подходы, методы и техники к решению практических задач в области психологии взаимодействия и саморегуляции ОПК-2.В.1 владеть навыками аргументации в процессе дискуссий, обсуждения профессиональных и других актуальных проблем ОПК-2.В.2 владеть социально-активным правомерным поведением в процессе реализации норм профессиональной этики и морали
Общепрофессиональные компетенции	*ОПК-3 Способен использовать общенаучные методы, законы физики, математический аппарат, методы моделирования и прогнозирования развития процессов и явлений при решении профессиональных задач	ОПК-3.З.1 знать основные понятия и законы естественных наук, методы математического анализа и моделирования ОПК-3.З.2 знать основные методы теоретического и экспериментального 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 выполнять технико-экономическое обоснование проектных решений по созданию систем обеспечения информационной безопасности, разрабатывать	ОПК-4.З.1 знать методики и инструменты экономической оценки эффективности проектных решений в области организации защиты информации ограниченного доступа ОПК-4.З.2 знать структуру и общий состав нормативных и методических документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и

	рабочую техническую документацию в соответствии с действующими нормативными и методическими документами в области защиты информации	экспортному контролю ОПК-4.У.1 уметь осуществлять обоснованный выбор проектных решений по организации защиты информации ограниченного доступа в соответствии с их технико-экономическим обоснованием ОПК-4.В.1 владеть навыками разработки технической проектной документации с учетом нормативных правовых актов, нормативных и методических документов при организации системы защиты информации
Общепрофессиональные компетенции	*ОПК-5 Способен планировать проведение работ по комплексной защите информации на объекте информатизации	ОПК-5.З.1 знать определение, цели и задачи комплексной системы защиты информации ОПК-5.З.2 знать внешние и внутренние угрозы информационной безопасности ОПК-5.З.3 знать особенности организационных и программно-аппаратных методик обеспечения информационной безопасности ОПК-5.У.1 уметь оценивать угрозы несанкционированного перехвата сведений по каналам передачи данных ОПК-5.У.2 уметь анализировать текущее состояние IT-инфраструктуры предприятия и прогнозировать изменения ее внешней и внутренней среды ОПК-5.В.1 владеть навыками своевременного обнаружения и устранения угроз информационной безопасности ОПК-5.В.2 владеть навыками восстановления информационных систем при повреждении ОПК-5.В.3 владеть навыками создания копий баз данных, критичных для предприятия
Общепрофессиональные компетенции	*ОПК-6 Способен применять положения теорий электрических цепей, радиотехнических сигналов, распространения радиоволн, цифровой обработки сигналов, информации и	ОПК-6.З.1 знать методы анализа электрических цепей при гармонических и произвольных воздействиях ОПК-6.З.2 знать принципы преобразования сигналов линейными и нелинейными цепями ОПК-6.З.3 знать устройство, принцип действия и характеристики типовых линейных и нелинейных устройств; типовые нелинейные цепи и преобразование ими радиосигналов ОПК-6.У.1 уметь рассчитывать

	кодирования, электрической связи для решения профессиональных задач	переходные процессы в линейных системах ОПК-6.У.2 уметь решать задачи по анализу и синтезу электрических цепей с использованием математических методов и вычислительной техники ОПК-6.В.1 владеть навыками анализа электрических цепей ОПК-6.В.2 владеть навыками расчета параметров радио-технических цепей
Общепрофессиональные компетенции	*ОПК-7 Способен применять программные средства системного и прикладного назначения, языки, методы и инструментальные средства программирования для решения профессиональных задач	ОПК-7.З.1 знать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности ОПК-7.У.1 уметь выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности ОПК-7.В.1 владеть навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности
Общепрофессиональные компетенции	*ОПК-8 Способен реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз	ОПК-8.З.1 знать основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области ОПК-8.З.2 знать физические основы образования каналов утечки информации и возможности технических средств перехвата информации, а также способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации ОПК-8.З.3 знать порядок проверки технических средств и объектов информатизации на наличие электронных устройств негласного получения информации и порядок организации защиты информации от утечки по техническим каналам на объектах информатизации и в объектах

		информатизации ОПК-8.З.4 знать порядок ввода объекта информатизации системы технической защиты информации в эксплуатацию, порядок проведения категорирования технических средств и систем и аттестации объектов информатизации требованиям безопасности информации, порядок сертификации технических средств защиты информации ОПК-8.У.1 уметь анализировать и оценивать угрозы информационной безопасности объекта информатизации ОПК-8.У.2 уметь применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем ОПК-8.В.1 владеть навыками работы с нормативными правовыми актами ОПК-8.В.2 владеть методами и средствами выявления угроз безопасности объекта информатизации, формирования требований по защите информации, методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов
Общепрофессиональные компетенции	*ОПК-9 Способен применять технологии получения, накопления, хранения, обработки, интерпретации и использования информации в ходе профессиональной деятельности	ОПК-9.З.1 знать способы передачи и обработки данных, модели данных, основные понятия и правила построения баз данных ОПК-9.З.2 знать специальные информационные технологии в профессиональной деятельности ОПК-9.У.1 уметь проектировать модели данных, сети и системы передачи и обработки информации ОПК-9.У.2 уметь интерпретировать данные представленные на естественном языке, аудио- и видеоинформацию ОПК-9.В.1 владеть навыками построения систем управления данными, извлечения информации из баз данных, ее анализа и использования в профессиональной деятельности ОПК-9.В.2 владеть навыками обоснованного выбора современных систем управления базами данных и обработки информации
Общепрофессиональные	*ОПК-10 Способен	ОПК-10.З.1 знать основные понятия,

компетенции	осуществлять аналитическую деятельность с последующим использованием данных при решении профессиональных задач	принципы и методы теории системного анализа и управления в целях применения в профессиональной сфере ОПК-10.З.2 знать технико-криминалистические методы и средства, тактические приемы производства следственных действий, формы организации и методику раскрытия и расследования отдельных видов и групп преступлений ОПК-10.З.3 знать характеристики коррупционного поведения ОПК-10.У.1 уметь анализировать предметную область как систему, выявляя ее составляющие и связи между ними, строить модели систем ОПК-10.У.2 уметь эффективно использовать при выполнении профессиональных задач специальные техники, применяемые в аналитической деятельности правоохранительных органов ОПК-10.У.3 уметь выявлять пробелы в информации, необходимой для решения профессиональных задач, и проектировать процессы по их устранению ОПК-10.У.4 уметь анализировать, выявлять, давать оценку коррупционному поведению и содействовать его пресечению ОПК-10.В.1 владеть навыками моделирования систем на основе методов системного анализа и управления в современных средах проектирования ОПК-10.В.2 владеть навыками критической оценки надежности источников информации и работы с информацией, полученной из разных источников ОПК-10.В.3 владеть приемами применения в профессиональной деятельности теоретических основ раскрытия и расследования преступлений
Общепрофессиональные компетенции	*ОПК-11 Способен использовать автоматизированные информационные системы в профессиональной	ОПК-11.З.1 знать процессы и модели жизненного цикла автоматизированных информационных систем ОПК-11.З.2 знать методы анализа предметной области и формирования требований к автоматизированным

	деятельности	системам в профессиональной деятельности ОПК-11.З.3 знать функциональные и технологические стандарты использования информационных систем в профессиональной деятельности ОПК-11.У.1 уметь разрабатывать концептуальную модель прикладной области ОПК-11.У.2 уметь проводить анализ и оценку автоматизированных систем в профессиональной деятельности ОПК-11.В.1 владеть навыками работы с инструментальными средствами моделирования предметной области ОПК-11.В.2 владеть навыками использования программных комплексов для решения прикладных задач в профессиональной деятельности
Общепрофессиональные компетенции	*ОПК-12 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ОПК-12.З.1 знать перспективные методы информационных технологий и искусственного интеллекта, направленных на разработку новых научно-технических решений ОПК-12.З.2 знать технологии, разработанные с использованием методов машинного обучения, способные решать задачи профессиональной деятельности ОПК-12.У.1 уметь применять современные информационные технологии и перспективные методы искусственного интеллекта для решения задач профессиональной деятельности ОПК-12.В.1 владеть навыками разработки алгоритмов решения задач в профессиональной деятельности
Профессиональные компетенции	*ПК-1 Способен принимать участие в создании системы защиты информации на объекте информатизации	ПК-1.З.1 знать средства разработки систем защиты информации объектов информатизации; требования нормативных документов и стандартов в области информационной безопасности ПК-1.У.1 уметь проектировать, разрабатывать, внедрять и эксплуатировать системы защиты информации ПК-1.В.1 владеть навыками поддержания требуемого уровня информационной безопасности объекта информатизации
Профессиональные компетенции	*ПК-2 Способен проводить контроль	ПК-2.З.1 знать технические и программные средства информационной

	работоспособности технических и программно-аппаратных средств обработки и защиты информации	безопасности, основы сетевых технологий и направления их совершенствования ПК-2.У.1 уметь использовать современные технические, математические и программные средства для решения профессиональных задач ПК-2.В.1 владеть современными технологиями, методами и моделями оценки эффективности технических и программно-аппаратных средств при разработке систем защиты информации
Профессиональные компетенции	*ПК-3 Способен осуществлять установку, настройку и эксплуатацию компонентов технических систем обеспечения безопасности информации и поддержку их работоспособного состояния	ПК-3.З.1 знать теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации ПК-3.З.2 знать порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях ПК-3.З.3 знать принципы организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации ПК-3.У.1 уметь осуществлять комплектование, конфигурирование, настройку компонентов технических систем обеспечения безопасности ПК-3.У.2 уметь организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней ПК-3.В.1 владеть навыками установки, настройки, администрирования и эксплуатации компонентов систем защиты информации ПК-3.В.2 владеть навыками диагностики и восстановления работоспособности компонентов систем защиты информации
Профессиональные компетенции	*ПК-4 Способен организовывать и проводить мероприятия по контролю за обеспечением защиты информации, в том числе сведений, составляющих государственную	ПК-4.З.1 знать понятие и содержание политики информационной безопасности, показатели качества и эффективности системы безопасности предприятия ПК-4.У.1 уметь выделять объекты защиты и строить концепцию информационной безопасности, регулировать меры по обеспечению информационной безопасности ПК-4.В.1 владеть навыками разработки

	тайну, проводить анализ эффективности системы защиты информации	положений, регламентов и процессов взаимодействия структурных элементов объекта информатизации
Профессиональные компетенции	*ПК-5 Способен осуществлять администрирование подсистем обеспечения информационной безопасности объекта информатизации	ПК-5.З.1 знать методы и инструментальные средства администрирования и контроля подсистем обеспечения информационной безопасности объекта информатизации ПК-5.У.1 уметь осуществлять мониторинг и периодический контроль функционирования средств и подсистем обеспечения информационной безопасности объекта информатизации ПК-5.В.1 владеть навыками использования инструментальных средств мониторинга и анализа состояния системы информационной безопасности
Профессиональные компетенции	*ПК-6 Способен применять технологии получения, накопления, хранения, обработки, анализа, интерпретации и использования информации в ходе профессиональной деятельности, работать с различными источниками информации, информационными ресурсами и технологиями; проводить информационно-поисковую работу с последующим использованием данных при решении профессиональных задач	ПК-6.З.1 знать способы сбора, предобработки, хранения, модификации данных ПК-6.У.1 уметь выбирать инструментальные средства для обработки данных в соответствии с поставленной задачей ПК-6.У.2 уметь собирать, анализировать и интерпретировать необходимую информацию, содержащуюся в различных формах отчетности и прочих источниках ПК-6.В.1 владеть методами программного анализа данных, необходимых для решения поставленных задач в ходе профессиональной деятельности ПК-6.В.2 владеть навыками выявления тенденций в динамике значений показателей объектов и процессов при решении профессиональных задач
Профессиональные компетенции	*ПК-7 Способен формировать и поддерживать в	ПК-7.З.1 знать назначение информационно-поисковых, логико-аналитических и экспертных систем, их

	актуальном состоянии автоматизированные базы и банки данных, использовать информационно-поисковые и логико-аналитические системы	тактико-технические характеристики и порядок применения в правоохранительных органах ПК-7.З.2 знать сущность и методики информационного и аналитического поиска, источники информации, необходимые для их осуществления ПК-7.З.3 знать понятие и структуру автоматизированной базы данных (программное обеспечение, банк данных, база знаний, система управления базами данных и т.д.) ПК-7.У.1 уметь разрабатывать модели данных, администрировать автоматизированные базы и банки данных ПК-7.В.1 владеть навыками освоения и внедрения в практику администрирования новых технологий работы с базами данных
Профессиональные компетенции	*ПК-8 Способен анализировать структуру и содержание информационных массивов и информационных процессов на предмет выявления угроз безопасности	ПК-8.З.1 знать методики проведения анализа оперативной обстановки, правила оформления результатов криминального анализа ПК-8.З.2 знать классификацию источников угроз и нарушителей информационной безопасности ПК-8.У.1 уметь проводить анализ вероятности реализации угрозы и ущерба от ее возникновения ПК-8.В.1 владеть навыками использования информационных сервисов для автоматизации прикладных и информационных процессов анализа систем защиты информации

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
10	9	6

4. ПРОГРАММА ГОСУДАРСТВЕННОГО ЭКЗАМЕНА

4.1. Программа государственного экзамена

4.1.1. Форма проведения ГЭ – *письменная*

4.1.2. Перечень компетенций, освоение которых оценивается на ГЭ приведен в таблице 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»
Математика. Аналитическая геометрия и линейная алгебра
Математика. Математический анализ
Основы теории информации
Дискретная математика
Техноэтика
Философия
Теория вероятностей
Вычислительная математика
УК-2 «Способен управлять проектом на всех этапах его жизненного цикла»
Экономика
Экономическое обоснование программных проектов
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
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»
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»
Физическая культура
Прикладная физическая культура (элективный модуль)
УК-10 «Способен формировать нетерпимое отношение к коррупционному поведению»
Правовая защита информации
Психология профессиональной деятельности
ОПК-1 «Способен на основе анализа основных этапов и закономерностей исторического развития Российского государства, его места и роли в контексте всеобщей истории формировать устойчивые внутренние мотивы профессионально-служебной деятельности, базирующиеся на гражданской позиции, патриотизме, ответственном отношении к выполнению профессионального долга»
Информационное право
Правовая защита информации
ОПК-2 «Способен анализировать мировоззренческие, социальные и личностно-значимые проблемы в целях формирования ценностных, этических основ профессионально-служебной деятельности»
Психология профессиональной деятельности
Профессиональная этика и служебный этикет
ОПК-3 «Способен использовать общенаучные методы, законы физики, математический аппарат, методы моделирования и прогнозирования развития процессов и явлений при решении профессиональных задач»
Информатика
Математика. Аналитическая геометрия и линейная алгебра
Математика. Математический анализ
Физика
Дискретная математика
Учебная практика
Алгоритмы и структуры данных
Вычислительная математика
Электроника и схемотехника
Электротехника
Математические основы обработки информации
Основы электро-, радиоизмерений
ОПК-4 «Способен выполнять технико-экономическое обоснование проектных решений по созданию систем обеспечения информационной безопасности, разрабатывать рабочую техническую документацию в соответствии с действующими нормативными и методическими документами в области защиты информации»
Учебная практика
Экономика
Организационная защита информации
Технологии защищенного документооборота
Управление информационной безопасностью
Экономическое обоснование программных проектов
ОПК-5 «Способен планировать проведение работ по комплексной защите информации на объекте информатизации»
Основы информационной безопасности
Учебная практика

Теория информационной безопасности и методология защиты информации
Программно-аппаратная защита информации
Управление информационной безопасностью
Производственная преддипломная практика
ОПК-6 «Способен применять положения теорий электрических цепей, радиотехнических сигналов, распространения радиоволн, цифровой обработки сигналов, информации и кодирования, электрической связи для решения профессиональных задач»
Основы радиотехники
Электротехника
Основы электро-, радиоизмерений
ОПК-7 «Способен применять программные средства системного и прикладного назначения, языки, методы и инструментальные средства программирования для решения профессиональных задач»
Учебная практика
Технологии и методы программирования
Программно-аппаратная защита информации
ОПК-8 «Способен реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз»
Основы информационной безопасности
Правовая защита информации
Теория информационной безопасности и методология защиты информации
Программно-аппаратная защита информации
Системы и сети передачи информации
Организационная защита информации
Техническая защита информации
Управление информационной безопасностью
ОПК-9 «Способен применять технологии получения, накопления, хранения, обработки, интерпретации и использования информации в ходе профессиональной деятельности»
Основы программирования
Технологии и методы программирования
Программно-аппаратная защита информации
Системы и сети передачи информации
Технологии защищенного документооборота
Управление информационной безопасностью
Производственная преддипломная практика
ОПК-10 «Способен осуществлять аналитическую деятельность с последующим использованием данных при решении профессиональных задач»
Информатика
Технологии и методы программирования
Психология профессиональной деятельности
Теория информационной безопасности и методология защиты информации
Программно-аппаратная защита информации
Производственная преддипломная практика
ОПК-11 «Способен использовать автоматизированные информационные системы в профессиональной деятельности»
Компьютерная графика
Программно-аппаратная защита информации
Организационная защита информации
Управление информационной безопасностью

Производственная преддипломная практика
ОПК-12 «Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности»
Технологии и методы программирования
Математические основы обработки информации
Производственная преддипломная практика
ПК-1 «Способен принимать участие в создании системы защиты информации на объекте информатизации»
Учебная практика
Производственная практика
Защита банковской информации
Защита от вредоносных программ
Технологии защиты от скрытой передачи данных
Технологии защиты электронных платежей
Предметно-ориентированные автоматизированные информационные системы
ПК-2 «Способен проводить контроль работоспособности технических и программно-аппаратных средств обработки и защиты информации»
Мультимедиа технологии
Технологии обработки аудио- и видеоданных
Безопасность вычислительных сетей
Безопасность инфокоммуникационных систем
Безопасность систем баз данных
Имитационное моделирование
Интеллектуальные системы и технологии
Моделирование систем
Производственная практика
Распознавание образов
ПК-3 «Способен осуществлять установку, настройку и эксплуатацию компонентов технических систем обеспечения безопасности информации и поддержку их работоспособного состояния»
Организация ЭВМ и вычислительных систем
Теория кодирования
Безопасность вычислительных сетей
Безопасность инфокоммуникационных систем
Производственная практика
ПК-4 «Способен организовывать и проводить мероприятия по контролю за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, проводить анализ эффективности системы защиты информации»
Защита банковской информации
Защита и обработка документов ограниченного доступа
Защита от вредоносных программ
Производственная практика
Технологии защиты от скрытой передачи данных
Технологии защиты электронных платежей
ПК-5 «Способен осуществлять администрирование подсистем обеспечения информационной безопасности объекта информатизации»
Защита банковской информации
Производственная практика
Технологии защиты электронных платежей
ПК-6 «Способен применять технологии получения, накопления, хранения, обработки, анализа, интерпретации и использования информации в ходе профессиональной

деятельности, работать с различными источниками информации, информационными ресурсами и технологиями; проводить информационно-поисковую работу с последующим использованием данных при решении профессиональных задач»
Учебная практика
Мультимедиа технологии
Теория кодирования
Технологии обработки аудио- и видеоданных
Безопасность систем баз данных
Методы и средства криптографической защиты информации
Имитационное моделирование
Интеллектуальные системы и технологии
Моделирование систем
Защита от вредоносных программ
Криминалистика
Правоохранительные органы
Распознавание образов
Технологии защиты от скрытой передачи данных
Информационно-аналитическое обеспечение правоохранительной деятельности
Компьютерная экспертиза
Криминология
Производственная преддипломная практика
ПК-7 «Способен формировать и поддерживать в актуальном состоянии автоматизированные базы и банки данных, использовать информационно-поисковые и логико-аналитические системы»
Учебная практика
Теория систем и системный анализ
Организация ЭВМ и вычислительных систем
Безопасность систем баз данных
Производственная практика
Имитационное моделирование
Моделирование систем
Комплексные системы защиты информации в правоохранительной сфере
Компьютерная экспертиза
Производственная преддипломная практика
ПК-8 «Способен анализировать структуру и содержание информационных массивов и информационных процессов на предмет выявления угроз безопасности»
Теория систем и системный анализ
Безопасность вычислительных сетей
Безопасность инфокоммуникационных систем
Безопасность систем баз данных
Основы уголовного права
Уголовный процесс
Административный процесс
Защита от вредоносных программ
Производственная практика
Технологии защиты от скрытой передачи данных
Комплексные системы защиты информации в правоохранительной сфере
Компьютерная экспертиза
Производственная преддипломная практика

4.1.3. Методические рекомендации обучающимся по подготовке к ГЭ.

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 Информационное право

Тема 1.1 Правовая защита информации
Тема 1.2 Интеллектуальная собственность
Тема 1.3 Защита персональных данных
Тема 1.4 Ответственность в информационной сфере
Тема 1.5 Информация с ограниченным доступом

Блок 2 Комплексные системы защиты информации (КСЗИ)

Тема 2.1 Методология построения КСЗИ
Тема 2.2 Организационная зашита информации
Тема 2.3 Техническая защита информации
Тема 2.4 Защита компьютерных сетей
Тема 2.5 Программно-аппаратная защита информации
Тема 2.6 Каналы утечки информации
Тема 2.7 Защита от скрытой передачи данных
Тема 2.8 Оценка эффективности КСЗИ

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.

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 специальностям 10.05.05, дипломные работы студентов должны отражать один или несколько видов профессиональной деятельности выпускников:

Укрупненная группа подготовки: 10.00.00 Информационная безопасность. Уровень высшего образования: специалитет. Специальность: 10.05.05 Безопасность

информационных технологий в правоохранительной сфере. Специализация: 10.05.05.01 Технологии защиты информации в правоохранительной сфере. Виды профессиональной деятельности выпускников:

- эксплуатационная
  - установка, настройка и поддержание в работоспособном состоянии компонентов технических систем обеспечения безопасности информации;
  - участие в проведении специальных проверок и исследований, аттестации объектов, помещений, технических средств, систем, сертификационных испытаний программных средств на предмет соответствия требованиям защиты информации;
  - администрирование систем обеспечения информационной безопасности на объекте.
- организационно-управленческая
  - организационно-правовое обеспечение деятельности по получению, накоплению, обработке, анализу, использованию информации и защите объектов информатизации, информационных технологий и ресурсов;
  - разработка и контроль эффективности осуществления системы мер по формированию и использованию информационных ресурсов, систем обеспечения информационной безопасности;
  - организация работы малых групп и коллективов исполнителей, сформированных для решения конкретных профессиональных задач.
- научно-исследовательская
  - сбор, изучение, систематизация и обобщение научно-технической информации, отечественного и зарубежного опята по проблемам информационно-аналитической работы и обеспечения защиты информации;
  - анализ прикладных проблем информационно-аналитического и информационно-психологического обеспечения безопасности информационных технологий;
  - разработка заданий, планов, программ проведения прикладных научных исследований и технических разработок;
  - проведение экспериментов по заданным методикам;
  - выполнение прикладных научных исследований, подготовка отчетов, докладов.
- проектно-технологическая;
  - сбор и анализ исходных данных для проектирования систем обработки и анализа информации с учетом необходимости ее защиты в соответствии с требованиями безопасности информации;
  - участие в проектировании систем, комплексов средств и технологий обработки и защиты информации, в разработке технологической документации;
  - адаптация к защищаемым объектам современных информационных технологий и методов обеспечения безопасности информации на основе отечественных и международных стандартов.
- педагогическая.
  - преподавание в организациях, осуществляющих образовательную деятельность, дисциплин (модулей) в области информационных технологий и информационной безопасности.

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)

Основная часть

Работа студента над ВКР по специальностям 10.05.05 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 10.05.05 «Безопасность информационных технологий в правоохранительной сфере» 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) построение модели угроз в рассматриваемой предметной области;
4) оценка и анализ рисков информационной безопасности;
5) реинжиниринг бизнес-процессов, построение диаграмм IDEF0 to-be, DFD to-be, UML-диаграмм и др., функционально-стоимостной и функционально-временной анализ;
6) выбор и обоснование средств зашиты информации и реализации построенных моделей. Описание их настройки;
7) разработка/адаптация политики информационной безопасности предприятия, включающей организационные, технические, программные и другие аспекты.
8) правовые вопросы защиты информации. Разработка рекомендаций и предложений в правовом аспекте;
9) экономическое обоснование проекта. Анализ результатов работы.

Для специальностей 10.05.05 «Безопасность информационных технологий в правоохранительной сфере» 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.

Объектами профессиональной деятельности выпускников по специальности 10.05.05 являются:

- информационные технологии и системы, а также информационные процессы и ресурсы в правоохранительной деятельности;
- технологии защиты информации и информационных ресурсов, обеспечения информационной безопасности объектов различного уровня (системы, объект системы, компонент объекта);
- объекты информатизации правоохранительных органов;
- организационно-правовые механизмы осуществления информационно-аналитической деятельности в правоохранительной сфере;
- судебно-экспертная деятельность в области компьютерной экспертизы;
- процессы управления системами, обеспечивающими информационную безопасность на защищаемых объектах, методы и средства оптимизации процессов управления.

В тексте основной части ВКР результаты проведения инжиниринга/реинжиниринга представляются в виде совокупности диаграмм (IDEFX, DFD, UML и т.п.). Диаграммы IDEFX, DFD и UML требуют обязательного описания связным текстом, который должен описывать суть отображаемых на диаграммах процессов, а не форму их отражения на диаграмме. Количество входных, выходных, управленческих стрелок и механизмов на IDEF0 диаграммах должно быть с одной стороны достаточным для описания полноты отображаемого процесса, а с другой не быть чрезмерным. В связи с этим приведем ниже рекомендации, которые следует учитывать при построении инфологических моделей и описании бизнес-процессов объектов исследования.

Прежде всего следует учитывать, что при описании защищаемых бизнес-процессов выбранная точка зрения на эти процессы не должна меняться от контекстного до низшего уровня декомпозиции. Как правило, такой точкой зрения в данном случае может быть точка зрения инженера по информационной безопасности, администратора ИБ, сетевого инженера, системного администратора или директора по информационной безопасности.

В качестве механизмов и ресурсов при разработке защищенных информационных систем могут использоваться конкретное аппаратное и программное обеспечение и, обязательно, людские ресурсы. Для правильного указания людских ресурсов следует помнить их распределение в ходе жизненного цикла проекта разработки информационной системы. Приведем ответы на основные вопросы, возникающие на укрупненных фазах проектирования.

Фаза 1. Определение назначения и функций информационной системы

Кто работает? Владельцы бизнес-процессов (руководители предприятий), бизнес-аналитики, директор и инженеры по информационной безопасности

Что они делают? Оценивают актуальность разработки системы (оценка потребности в данной системы и оценка бизнес-рисков (финансовых, репутационных, социальных, политических)

Как предоставляют результат? Формируют стратегические (верхние) уровни декомпозиции диаграмм бизнес-процессов и диаграмм потоков данных AS-IS и TO-BE (либо UML-диаграммы), разрабатывают документ по стратегии, выявляют критические элементы (активы), формируют модель нарушителей и модель угроз, политику безопасности предприятия

Кому передают результаты? Архитекторам системы, системным аналитикам, инженерам по безопасности

Фаза 2. Системный анализ бизнес-процессов

Кто работает? Владельцы бизнес-процессов (руководители подразделений предприятий), архитекторы системы, системные-аналитики, инженеры по информационной безопасности

Что они делают? Выбирают и обосновывают методологию и инструмент проведения системного анализа (структурный (например, BPwin) или объектно-ориентированный (например, UML)), проводят детальный системный анализ бизнес-процессов, оценивают защищенность РИС

Как предоставляют результат? Формируют декомпозиции диаграмм бизнес процессов и диаграмм потоков данных AS-IS и TO-BE, уточняют документ по стратегии, уточняют политику безопасности предприятия, формируют частные политики безопасности и профили защиты

Кому передают результаты? Системным программистам, инженерам по безопасности

Фаза 3. Проектирование архитектуры системы

Кто работает? Архитекторы системы, системные-программисты, инженеры по информационной безопасности

Что они делают? Выбирают и обосновывают методологию и инструмент построения моделей и структур данных (реляционная (например, ERwin),объектно-реляционная (например, EFW), сервис-ориентированная (SOAP), агентная), разрабатывают архитектуру системы, проводят имитационное моделирование системы, обосновывают выбор платформы для системы, определяют периметры защиты и оценивают защищенность РИС

Как предоставляют результат? Формируют диаграммы моделей и структур данных (сущностей) логического уровня (ERD или ORM TO-BE), уточняют документ по стратегии, уточняют политику безопасности предприятия, и частные политики безопасности, формируют задание по безопасности

Кому передают результаты? Администраторам баз данных, прикладным программистам, инженерам по безопасности

Фаза 4. Проектирование баз данных системы

Кто работает? Архитекторы системы, системные-программисты, администраторы баз данных, прикладные программисты, инженеры по информационной безопасности

Что они делают? Выбирают и обосновывают тип СУБД (локальная, клиент-серверная, многоуровневая, распределенная), разрабатывают логические и физические модели данных, распределяют и обосновывают роли доступа к данным, определяют периметры защиты и оценивают защищенность РИС

Как предоставляют результат? Формируют диаграммы моделей и структур данных (сущностей) логического и физического уровня, уточняют документ по стратегии, уточняют политику безопасности предприятия, и частные политики безопасности, формируют задание по безопасности

Кому передают результаты? Прикладным программистам, инженерам по безопасности, администраторам баз данных, системным администраторам, администраторам по безопасности

Фаза 5. Проектирование приложений доступа к данным

Кто работает? Системные-программисты, администраторы баз данных, прикладные программисты, инженеры и администраторы по информационной безопасности

Что они делают? Выбирают и обосновывают IDE, разрабатывают ограничения на доступ к данным, определяют эшелоны защиты, разрабатывают приложения доступа к данным, выбирают средства защиты информации СЗИ

Как предоставляют результат? Формируют диаграммы классов, программные единицы (программные проекты, модули. библиотеки), разрабатывают сопроводительную документацию и руководства пользователей системы

Кому передают результаты? Тестерам, техническим писателям, инженерам по безопасности, администраторам баз данных, системным администраторам, администраторам по безопасности

Фаза 6. Тестирование системы

Кто работает? Тестеры, системные-программисты, администраторы баз данных, прикладные программисты, инженеры и администраторы по информационной безопасности, пен-тестеры (тестеры на проникновение)

Что они делают? Выбирают и обосновывают методологию тестирования, проводят внутреннее тестирование (тестирование модулей системы, интеграционное тестирование, нагрузочное тестирование, комплексное тестирование, тестирование на наличие уязвимостей) и внешнее (с участием и на стороне заказчика) тестирование системы, разрабатывают регламенты мониторинга и аудита системы, выбирают средства мониторинга и аудита

Как предоставляют результат? Разрабатывают планы тестирования, формируют аналитические отчеты по результатам тестирования системы, подписывают акты тестирования, разрабатывают шаблоны регламентов мониторинга и аудита системы

Кому передают результаты? Результаты внутреннего тестирования -Разработчикам системы, результаты внешнего тестирования – разработчикам и заказчикам системы

Фаза 7. Внедрение системы

Кто работает? Тестеры, системные-программисты, прикладные программисты, инженеры и администраторы по информационной безопасности, администраторы баз данных, системны администраторы, сетевые администраторы, представители заказчика

Что они делают? Выбирают и обосновывают методологию внедрения («жесткая» или «мягкая»), разрабатывают план внедрения системы, проводят закупку необходимого ПО и АО, монтируют оборудование, разворачивают ПО и настраивают параметры системы, интегрируют систему со взаимодействующими системами предприятия.

Как предоставляют результат? Разрабатывают планы внедрения, формируют аналитические отчеты по результатам внедрения системы, подписывают акты приемо-сдаточных работ

Кому передают результаты? Разработчикам (директору проекта) и заказчикам системы (руководителям предприятия)

Фаза 8. Сопровождение системы

Кто работает? Системные администраторы, сетевые администраторы, администраторы баз данных, администраторы по информационной безопасности

Что они делают? Поддерживают работоспособность системы, адаптируют систему в соответствии с потребностями бизнеса, обновляют версии системы, обеспечивают целостность, доступность и конфиденциальность данных, устраняют уязвимости, формируют аналитические отчеты мониторинга и аудита системы, выбирают средства мониторинга и аудита

Как предоставляют результат? Формируют планы закупок ПО и АО для бесперебойного функционирования системы при ее адаптации, формируют аналитические отчеты по результатам мониторинга и аудита системы, актуализируют и обновляют политики информационной безопасности

Кому передают результаты? Руководителям предприятия

Формулировка назначения системы – это ОДНО предложение, обязательно содержащие подлежащее (с указанием собственного имени системы), сказуемое и прямое дополнение, отражающее суть автоматизируемого бизнес процесса.

Например, назначение системы AirLogger может быть сформулировано следующим образом: «Система AirLogger предназначена для оценки реализации студентом информационной безопасности его учебных проектов».

Текст основной части ВКР должен содержать структурную схему архитектуры системы с указанием актуализированных угроз (например, рис. 2.13), а также таблицу «Актуальные угрозы безопасности информации», включающую:

- наименование угрозы безопасности информации;
- возможности нарушителя по реализации угрозы;
- используемые уязвимости информационной системы;
- описание способов реализации угрозы безопасности информации;
- объекты воздействия (активы);
- возможные результат и последствия от реализации угрозы безопасности информации (риски).

5.2. Дополнительные компоненты ВКР определяемые выпускающей кафедрой.

Определения, обозначения и сокращения

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

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

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

Пример

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

Недопустимо использовать следующие сокращения:

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

Введение

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

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

Заключение

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

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

В заключении не должно содержаться цитат и прочих текстовых заимствований.

Список использованных источников

Можно использовать заголовки:

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

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

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

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

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

Порядок сортировки источников должен быть следующим:

- международные нормативные акты;
- конституция Российской Федерации;
- нормативно-правовые документы:
    - Федеральные конституционные законы
    - Постановления конституционного суда
    - Кодексы
    - Федеральные законы
    - Законы
    - Указы Президента РФ
    - Акты Правительства
        - Постановления
        - Распоряжения
- Акты Верховного и Высшего Арбитражного Судов.
- Нормативные акты министерств и ведомств
    - Постановления
    - Приказы
    - Распоряжения
    - Письма
- Региональные нормативные акты
- ГОСТы
- СНиПы, СП, ЕНИРы, ТУ
- книги, учебные пособия, статьи, монографии, электронные источники (CD-диски, ссылки из Интернета)

- иностранные источники.

Список использованных источников в каждом подразделе может составляться:

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

Приложения

Приложения к дипломной работе по специальностям 10.05.05 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 10.05.05 рекомендуется следующая структура иллюстративно-графического материала:

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

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

3. Слайд, содержащий цель и задачи работы.

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

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

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

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

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

Слайды в обязательном порядке должны быть пронумерованы.

Существуют следующие рекомендации по оформлению слайдов:

- все слайды должны быть выдержаны в едином стиле, рекомендуется использовать один-два оттенка цвета, один тип шрифта, а также одинаковый размер шрифта для заголовков и один размер для основного текста.
- используемые цветовые гаммы должны быть максимально контрастными – черный шрифт на белом фоне или белый шрифт на черном фоне. Размер шрифта должен быть достаточен для «читаемости» слайда (как правило, не менее 18 пт.).
- рекомендуется свести к минимуму эффекты анимации, так как они значительно усложняют и удлиняют процесс защиты.
- крайне нежелательно дублировать на слайдах текст, произносимый студентов в докладе (кроме цели и задач работы и заключения). Информация на слайдах должна дополнять доклад, в основном с помощью графического, иллюстративного материала, а также формул и таблиц. Большие блоки текста на слайдах бесполезны.
- нумерация рисунков, диаграмм таблиц и схем может проводится независимо от их номеров в тексте ВКР, начиная с номера 1.

при представлении больших таблиц на слайдах необходимо проанализировать возможность их разделения на несколько мелких.

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

Защита ВКР (за исключением работ, содержащих сведения, составляющие государственную тайну) проводится на открытом заседании ГЭК с участием не менее двух третей её состава в установленное расписанием время. Кроме членов ГЭК на защите могут присутствовать другие лица: обучающиеся, представители заинтересованных предприятий, организаций, учреждений, руководители ВКР, консультанты, преподаватели и др. Председатель ГЭК имеет право удалить сторонних лиц при нарушении ими порядка проведения защиты ВКР. При проведении защиты ВКР, по решению председателя ГЭК, может проводиться видеозапись. Перед началом проведения защиты ВКР председатель ГЭК уведомляет присутствующих о проведении видеозаписи.

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

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

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

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

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

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

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

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

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

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

Рекомендуемая структура доклада для специальностей 10.05.05 приведена в таблице 1.

Таблица 1 – Общая структура доклада на защите ВКРС

№ п.п.	Специальность 10.05.03
1	Актуальность темы работы
2	Цель и задачи работы
3	Результаты аналитического поиска существующих решений
4	Анализ предметной области
5	Инжиниринг/Реинжиниринг бизнес-процессов
6	Архитектура разрабатываемой системы
7	Используемые средства, методы и технологии
8	Структура базы данных
9	Вопросы информационной безопасности и защиты информации
10	Оценка эффективности предлагаемых решений
11	Выводы по работе

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

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

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

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

При ответах на вопросы членов ГЭК следует учитывать следующее:

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

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

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

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

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

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

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

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

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

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

Завершенная и переплетенная ВКР представляется студентом руководителю ВКР на рассмотрение в срок не позднее 15 календарных дней до предполагаемой даты защиты, которая определяется на основании расписания государственных аттестационных испытаний. Не позднее 10 календарных дней до предполагаемой даты защиты, руководитель подготавливает отзыв (рис. 2.3), а также ставит подпись на титульном листе ВКР. При выявленном недопустимым объеме неправомерных заимствований, руководитель отметит этот факт в отрицательном отзыве. *После получения отзыва руководителя вносить изменения в текст ВКР недопустимо!*

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

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

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

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

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

- это должен быть один файл формата PDF с установленной защитой от копирования;
- файл должен иметь имя формата ГОД_МЕСЯЦ_№ГРУППЫ_ФамилияИО.pdf (например, 2021_06_3643_ИвановИИ.pdf);
- файл должен содержать текст ВКР и сканированные копии титульного листа, листа задания, отзыва руководителя и рецензии.

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

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

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

6. ПОРЯДОК ПОДАЧИ И РАССМОТРЕНИЯ АПЕЛЛЯЦИИ ПО РЕЗУЛЬТАТАМ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

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

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

7.1. Основная литература

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

Таблица 4 – Перечень печатных и электронных учебных изданий

Шифр/ URL адрес	Библиографическая ссылка	Количество экземпляров в библиотеке (кроме электронных экземпляров)
37 **Г 72**	Государственная итоговая аттестация : методические указания по подготовке к государственному экзамену и написанию и защите выпускной квалификационной работы / С.-Петерб. гос. ун-т аэрокосм. приборостроения ; сост.: С. Г. Фомичева, Т. Н. Елина, В. А. Мыльников. - Санкт-Петербург : Изд-во ГУАП, 2021. - 79 с. : рис., табл. - Библиогр.: с. 79 (10 назв.). - Б. ц. - Текст : непосредственный.	5
004 **Б 24**	**Баранова, Е. К.** Моделирование системы защиты информации. Практикум : учебное пособие / Е. К. Баранова, А. В. Бабаш. - 2-е изд., перераб. и доп. - М. : РИОР : ИНФРА-М, 2018. - 224 с.	5
004 **Б 90**	**Бузов, Г. А.** Защита информации ограниченного доступа от утечки по техническим каналам / Г. А. Бузов. - М. : Горячая линия - Телеком, 2017. - 586 с.	5
004 **Б 39**	**Беззатеев, Сергей Валентинович** (д-р техн. наук, доц.). Программирование задач по обеспечению информационной безопасности : лабораторный 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. Бакай ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - Санкт-Петербург : Изд-во ГУАП, 2020. - 133 с.	5

004 **Т 23**	**Татарникова, Татьяна Михайловна** (проф.). Анализ данных в прикладных задачах обеспечения информационной безопасности : монография / Т. М. Татарникова ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - СПб. : Изд-во ГУАП, 2018. - 115 с.	5
004 **И 98**	**Ищейнов, В. Я.** Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации : учебное пособие / В. Я. Ищейнов, М. В. Мецатунян. - 2-е изд., перераб. и доп. - М. : ФОРУМ : ИНФРА-М, 2017. - 256 с.	5
004 **З-40**	**Защита информации** : учебное пособие / А. П. Жук [и др.]. - 2-е изд. - М. : РИОР : ИНФРА-М, 2017. - 392 с.	5
338 **К 22**	**Карзаева, Н. Н.** Основы экономической безопасности : учебник / Н. Н. Карзаева. - М. : ИНФРА-М, 2019. - 275 с.	5
004 **О-35**	**Овчинников, Андрей Анатольевич** (канд. техн. наук, доц.). Основы информационной безопасности. Исторические шифры : учебно-методическое пособие / А. А. Овчинников ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - СПб. : Изд-во ГУАП, 2018. - 40 с.	5
004 **Ш 22**	**Шаньгин, В. Ф.** Информационная безопасность и защита информации / В. Ф. Шаньгин. - М. : ДМК Пресс, 2017. - 702 с.	5
004.4 **И 46**	**Ильина, Дарья Викторовна**. Проектирование и разработка безопасных веб-приложений : учебное пособие / Д. В. Ильина ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - Санкт-Петербург : Изд-во ГУАП, 2019. - 43 с.	5

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. 13-15

10. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

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

10.1.1. Состав оценочных средств приведен в таблице 7.

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

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

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

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

Описание показателей для оценки индикаторов достижения компетенций для ГЭ:

– способность последовательно, четко и логично излагать материал программы дисциплины;

– умение справляться с задачами;

– умение формулировать ответы на вопросы в рамках программы ГЭ с использованием материала научно-методической и научной литературы;

– уровень правильности обоснования принятых решений при выполнении практических задач.

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

Для оценки критериев уровня сформированности (освоения) компетенций студентами при проведении ГЭ в формах «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 IDEF0, DFD, ER. Процесс принятия решений в области обеспечения информационной безопасности автоматизированных систем. Инфологическое моделирование. Цели, задачи, методы.	*УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий
2	Проектная и операционная деятельность.	*УК-2 Способен управлять

	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.	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	Международные стандарты информационной безопасности Развитие системы официальных взглядов на обеспечение нацбезопасности государства в информационной сфере	*УК-5 Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия
6	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
7	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
8	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
9	Методы и модели оценки экономической эффективности проекта по разработке и	*УК-9 Способен принимать обоснованные экономические

	внедрению системы информационной безопасности Экономический подход к оценке эффективности комплексных систем защиты информации	решения в различных областях жизнедеятельности
10	Особенности профилактики коррупционных преступлений, совершаемых в правоохранительных органах	*УК-10 Способен формировать нетерпимое отношение к коррупционному поведению
11	Основные направления государственной политики в сфере информатизации. Нормативные документы Правоотношения в сфере правовой защиты информации Понятие, признаки правоотношений в сфере правовой защиты информации и их юридическая природа Понятие и признаки субъектов защиты прав интеллектуальной собственности Содержание правоотношений в сфере защиты прав интеллектуальной собственности Способы защиты личных неимущественных прав	*ОПК-1 Способен на основе анализа основных этапов и закономерностей исторического развития Российского государства, его места и роли в контексте всеобщей истории формировать устойчивые внутренние мотивы профессионально-служебной деятельности, базирующиеся на гражданской позиции, патриотизме, ответственном отношении к выполнению профессионального долга
12	Понятие правовой защиты информации Цели правовой защиты информации Правовая основа правовой защиты информации Принципы правовой защиты информации: понятие, система, место в системе принципов права Объекты правоотношений в сфере правовой защиты информации: понятие, признаки, виды	*ОПК-2 Способен анализировать мировоззренческие, социальные и личностно-значимые проблемы в целях формирования ценностных, этических основ профессионально-служебной деятельности
13	Математическая модель шифра. Математические основы обработки информации в задачах информационной безопасности. Модулярная арифметика. Кольца вычетов.	*ОПК-3 Способен использовать общенаучные методы, законы физики, математический аппарат, методы моделирования и прогнозирования развития процессов и явлений при решении профессиональных задач
14	Проектная документация. Назначение, состав и классификация. Технико-экономическое обоснование проектных решений	*ОПК-4 Способен выполнять технико-экономическое обоснование проектных решений по созданию систем обеспечения информационной безопасности, разрабатывать рабочую техническую документацию в соответствии с действующими нормативными и методическими документами в области защиты информации
15	Цели, задачи и принципы построения комплексных систем защиты информации	*ОПК-5 Способен планировать проведение работ по

	Методологические основы организации комплексных систем защиты информации Разработка политики безопасности предприятия	комплексной защите информации на объекте информатизации
16	Технические каналы утечки информации, их классификация	*ОПК-6 Способен применять положения теорий электрических цепей, радиотехнических сигналов, распространения радиоволн, цифровой обработки сигналов, информации и кодирования, электрической связи для решения профессиональных задач
17	Классификация информационных технологий. Виды системного и прикладного программного обеспечения. Отечественные SIEM-системы. Особенности настройки и применения.	*ОПК-7 Способен применять программные средства системного и прикладного назначения, языки, методы и инструментальные средства программирования для решения профессиональных задач
18	Состав, объекты и степень конфиденциальности защищаемой информации. Особенности защиты речевой информации Механизмы обеспечения безопасности информации Методика выявления нарушителей, тактики их действий и состава интересующей их информации	*ОПК-8 Способен реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз
19	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-9 Способен применять технологии получения, накопления, хранения, обработки, интерпретации и использования информации в ходе профессиональной деятельности
20	Сущность и задачи информационно-аналитической деятельности в правоохранительных органах.	*ОПК-10 Способен осуществлять аналитическую деятельность с последующим использованием данных при решении профессиональных задач
21	Понятие инженерии программирования.	*ОПК-11 Способен

	Вопросы и задачи инженерии программирования Состав и структура информационных систем, основные элементы, порядок функционирования Современные технологии проектирования информационных систем	использовать автоматизированные информационные системы в профессиональной деятельности
22	Цели, задачи и принципы построения комплексных систем защиты информации Цели и задачи защиты информации в автоматизированных системах Системный структурный анализ – основа методологии проектирования информационных систем	*ОПК-12 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности
23	Реинжиниринг бизнес-процессов Понятие проектирования информационных систем. Состав проекта Проектирование системы зашиты информации для существующей автоматизированной системы	*ПК-1 Способен принимать участие в создании системы защиты информации на объекте информатизации
24	Требования, предъявляемые к комплексным системам защиты информации Угрозы безопасности информации.	*ПК-2 Способен проводить контроль работоспособности технических и программно-аппаратных средств обработки и защиты информации
25	Общая характеристика задач моделирования КСЗИ Формальные модели безопасности и их анализ. Прикладные модели защиты информации в АС. Формализация модели безопасности. Показатель уровня защищенности, основанный на экспертных оценках.	*ПК-3 Способен осуществлять установку, настройку и эксплуатацию компонентов технических систем обеспечения безопасности информации и поддержку их работоспособного состояния
26	Модели нарушителей безопасности АС Особенности синтеза средств защиты информации автоматизированных систем от несанкционированного доступа	*ПК-4 Способен организовывать и проводить мероприятия по контролю за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, проводить анализ эффективности системы защиты информации
27	Модели нарушителей безопасности АС. Методика выявления нарушителей, тактики их действий и состава интересующей их информации Обеспечение безопасности информации в непредвиденных ситуациях.	*ПК-5 Способен осуществлять администрирование подсистем обеспечения информационной безопасности объекта информатизации
28	Особенности помещений как объектов защиты для работы по защите информации Особенности синтеза СЗИ АС от НСД	*ПК-6 Способен применять технологии получения, накопления, хранения,

	Методика синтеза СЗИ Оптимальное построение системы защиты для АС Проектирование системы зашиты информации для существующей АС	обработки, анализа, интерпретации и использования информации в ходе профессиональной деятельности, работать с различными источниками информации, информационными ресурсами и технологиями; проводить информационно-поисковую работу с последующим использованием данных при решении профессиональных задач
29	Специальные информационно-поисковые технологии в правоохранительной сфере Специализированные базы знаний	*ПК-7 Способен формировать и поддерживать в актуальном состоянии автоматизированные базы и банки данных, использовать информационно-поисковые и логико-аналитические системы
30	Принципы работы DLP-систем. Мониторинг инцидентов Принципы работы SIEM-систем. Анализ угроз информационной безопасности	*ПК-8 Способен анализировать структуру и содержание информационных массивов и информационных процессов на предмет выявления угроз безопасности

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 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	ПК-6, ПК-7

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

	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.	

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

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

10.2. Средства измерения индикаторов достижения компетенций для оценки защиты ВКР.

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

Описание показателей для оценки индикаторов достижения компетенций для ВКР и ее защиты:

- актуальность темы ВКР;
- научная обоснованность предложений и выводов;
- использование производственной информации и методов решения инженерно–технических, организационно-управленческих и экономических задач;
- теоретическая и практическая значимость результатов работы и/или исследования;
- полнота и всестороннее раскрытие темы ВКР;
- соответствие результатов работы и/или исследования, поставленной цели и задачам в ВКР;
- соответствие оформления ВКР установленным требованиям;
- умение четко и ясно изложить содержание ВКР;
- умение обосновать и отстаивать принятые решения;
- умение отвечать на поставленные вопросы;
- знание передового отечественного и зарубежного опыта;

– уровень самостоятельности выполнения работы и обоснованность объема цитирования;

– другое (уровень экономического обоснования, знание законодательных и нормативных документов, методических материалов по вопросам, касающимся конкретного направления).

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

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

Таблица 12 –Критерии оценки уровня сформированности компетенций

Оценка компетенции 5-балльная шкала	Характеристика сформированных компетенций
«отлично»	– студент глубоко и всесторонне усвоил учебный материал ОП, уверенно, логично, последовательно и грамотно его излагает; – опираясь на знания основной и дополнительной литературы, студент свободно увязывает усвоенные научные положения к практической деятельности, обосновывая выдвинутые предложения; – студент умело обосновывает и аргументирует выбор темы ВКР и выдвигаемые им идеи; – студент аргументированно делает выводы; – прослеживается четкая корреляционная зависимость между поставленными целью и задачами и полученными результатами работы и/или исследования; – студент свободно владеет системой специализированных понятий; – содержание доклада, иллюстративно–графического материала (при наличии) студента полностью соответствует содержанию ВКР; – студент соблюдает требования к оформлению ВКР и иллюстративно–графического материала (при наличии); – студент четко выделяет основные результаты своей профессиональной деятельности и обосновывает их теоретическую и практическую значимость; – студент строго придерживается регламента выступления; – студент ясно и аргументировано излагает материалы доклада; – присутствует четкость в ответах студента на поставленные членами государственной экзаменационной комиссии (ГЭК) вопросы; – студент точно и грамотно использует профессиональную терминологию при защите ВКР.
«хорошо»	– студент всесторонне усвоил учебный материал ОП, логично, последовательно и грамотно его излагает; – опираясь на знания основной и дополнительной литературы, студент привязывает усвоенные научные положения к практической деятельности, обосновывая выдвинутые предложения; – студент грамотно обосновывает выбор темы ВКР и выдвигаемые им идеи; – студент обоснованно делает выводы;

Оценка компетенции 5-балльная шкала	Характеристика сформированных компетенций
	– прослеживается зависимость между поставленными целью и задачами и полученными результатами работы и/или исследования; – студент владеет системой специализированных понятий; – содержание доклада и иллюстративно–графического материала(при наличии) студента соответствует содержанию ВКР; – студент соблюдает требования к оформлению ВКР и иллюстративно–графического материала(при наличии); – студент выделяет основные результаты своей профессиональной деятельности и обосновывает их теоретическую и практическую значимость; – студент придерживается регламента выступления; – студент ясно излагает материалы доклада; – присутствует логика в ответах студента на поставленные членами ГЭК вопросы; – студент грамотно использует профессиональную терминологию при защите ВКР.
«удовлетворительно»	– студент слабо усвоил учебный материал ОП, при его изложении допускает неточности; – опираясь на знания только основной литературы, студент привязывает научные положения к практической деятельности направления, выдвигая предложения; – студент слабо и не уверенно обосновывает выбор темы ВКР и выдвигаемые им идеи; – студент неаргументированно делает выводы и заключения; – не прослеживается зависимость между поставленными целью и задачами и полученными результатами работы и/или исследования; – студент плохо владеет системой специализированных понятий; – содержание доклада и иллюстративно–графического материала (при наличии) студента не полностью соответствует содержанию ВКР; – студент допускает ошибки при оформлении ВКР и иллюстративно–графического материала (при наличии); – студент слабо выделяет основные результаты своей профессиональной деятельности и не обосновывает их теоретическую и практическую значимость; – студент отступает от регламента выступления; – студент сбивчиво и неуверенно излагает материалы доклада; – отсутствует логика в ответах студента на поставленные членами ГЭК вопросы; – студент неточно использует профессиональную терминологию при защите ВКР.
«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;

Оценка компетенции 5-балльная шкала	Характеристика сформированных компетенций
	– 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.

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

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

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

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

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

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

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

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

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

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

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

36. Программные модели каналов утечки информации с объекта защиты.

37. Криптографические методы защиты на основе избыточности информации.

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

39. Разработка защищенной БД на предприятии.

Приложение № 2

Рецензия на программу государственной итоговой аттестации по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере» от работодателя

ПОЛИКОМ про

РЕЦЕНЗИЯ

на программу государственной итоговой аттестации

по программе специалитета 10.05.05

«Безопасность информационных технологий в правоохранительной сфере»

специализация «Организация и технологии защиты информации (в информационных системах)»

Представленная для рецензирования рукопись Программы государственной итоговой аттестации по программе высшего образования по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере», специализации «Организация и технологии защиты информации (в информационных системах)», 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 10.05.05 «Безопасность информационных технологий в правоохранительной сфере» (зарегистрирован Минюстом России 22 декабря 2021 г., регистрационный № 61703), 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.

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 10.05.05 «Безопасность информационных технологий в правоохранительной сфере», специализации «Организация и технологии защиты информации (в информационных системах)», 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.

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