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

Кафедра № 34

«УТВЕРЖДАЮ»
Проректор по
учебно–воспитательной работе

_____ В. М. Боер
(инициалы, фамилия)

«25» мая 2018

# ПРОГРАММА ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

| | |
|---|---|
| Код специальности | 10.05.03 |
| Наименование специальности | Информационная безопасность автоматизированных систем |
| Наименование специализации | Обеспечение информационной безопасности распределенных информационных систем |
| Форма обучения | очная |

Санкт–Петербург 2018 г

**Лист согласования**

Программу составил(а)

Зав.каф. проф.,д.т.н.,доц.  С.В. Беззатеев

(должность, уч. степень, звание) (подпись, дата) (инициалы, фамилия)

Программа одобрена на заседании кафедры № 34

«24» мая 2018 г, протокол № 10

Заведующий кафедрой № 34

д.т.н.,доц.  С.В. Беззатеев

должность, уч. степень, звание подпись, дата инициалы, фамилия

Ответственный за ОП 10.05.03(07)

доц.,к.т.н., доц.  В.А. Мыльников

должность, уч. степень, звание подпись, дата инициалы, фамилия

Заместитель директора института (факультета) № 3 по методической работе

доц.,к.т.н.,доц. М.В. Бураков

должность, уч. степень, звание подпись, дата инициалы, фамилия

# 1 ЦЕЛИ, ЗАДАЧИ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

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

1.2. Задачами ГИА являются:

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

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

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

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

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

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

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

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

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

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

знать – методы и средства физической культуры

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

владеть навыками – физических упражнений;

иметь опыт деятельности – в обеспечении физических тренировок;

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

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

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

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

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

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

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

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

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

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

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

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

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

*ПК-2 «способность создавать и исследовать модели автоматизированных систем»;

*ПК-3 «способность проводить анализ защищенности автоматизированных систем»;

*ПК-4 «способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы»;

*ПК-5 «способность проводить анализ рисков информационной безопасности автоматизированной системы»;

*ПК-6 «способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности»;

*ПК-7 «способность разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ»;

*ПК-8 «способность разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем»;

*ПК-9 «способность участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности»;

*ПК-10 «способность применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности»;

*ПК-11 «способность разрабатывать политику информационной безопасности автоматизированной системы»;

*ПК-12 «способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы»;

*ПК-13 «способность участвовать в проектировании средств защиты информации автоматизированной системы»;

*ПК-14 «способность проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации»;

*ПК-15 «способность участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты автоматизированных систем»;

*ПК-16 «способностью участвовать в проведении экспериментально-исследовательских

работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации»;

*ПК-17 «способность проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации»;

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

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

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

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

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

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

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

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

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

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

*ПК-28 «способность управлять информационной безопасностью автоматизированной системы»:

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

уметь – определять уровень освоения дисциплин;

владеть навыками – оценки результаты образовательного процесса;

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

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

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

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

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

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

знать – правила и этапы проектирования информационных систем;

уметь – проектировать структуру и состав информационной системы;

владеть навыками – выбора способа реализации информационной системы;

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

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

## 2 ФОРМЫ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

ГИА проводится в форме:

- государственный экзамен (ГЭ);
- защита выпускной квалификационной работы (ВКР).

## 3 ОБЪЕМ И ПРОДОЛЖИТЕЛЬНОСТЬ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

Объем и продолжительность ГИА указаны в таблице 1.

Таблица 1 – Объем и продолжительность ГИА

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

## 4 ПРОГРАММА ГОСУДАРСТВЕННОГО ЭКЗАМЕНА

4.1. Программа государственного экзамена.

4.1.1. Форма проведения ГЭ – письменная.

4.1.2. Перечень компетенций, освоение которых оценивается на ГЭ, приведен в таблице 2.

Таблица 2.1 – Перечень компетенций, уровень освоения которых оценивается на ГЭ

| |
|---|
| ОК-1 «способность использовать основы философских знаний для формирования мировоззренческой позиции» |
| Культурология |
| Философия |
| Психология и педагогика |
| Социальная психология |
| Социология и политология |
| ОК-2 «способность использовать основы экономических знаний в различных сферах деятельности» |
| Экономика |
| Международный бизнес |
| Мировая экономика |
| Защита банковской информации |
| Прикладная экономика |
| Технологии защиты электронных платежей |
| Основы управленческой деятельности |
| Экономика проектов в информационных технологиях |
| ОК-3 «способность анализировать основные этапы и закономерности исторического развития России, её место и роль в современном мире для формирования гражданской позиции и развития патриотизма» |

| |
|---|
| История |
| Правоведение |
| ОК-4 «способность использовать основы правовых знаний в различных сферах деятельности» |
| Социология и политология |
| Правоведение |
| ОК-5 «способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики» |
| Введение в специальность |
| Информационные технологии |
| Теория информации |
| Стандарты информационной безопасности |
| Основы управленческой деятельности |
| Управление информационной безопасностью |
| Организационное и правовое обеспечение информационной безопасности |
| Информационная безопасность распределенных информационных систем |
| ОК-6 «способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия» |
| История |
| Философия |
| Социальная психология |
| Психология и педагогика |
| Защита информации в распределенных информационных системах |
| Проектирование безопасных информационных систем |
| Основы управленческой деятельности |
| Управление информационной безопасностью |
| Научно-технический семинар |
| Научно-исследовательская работа |
| ОК-7 «способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности» |
| Экология |
| Экономика |
| Иностранный язык |
| Введение в специальность |
| Промышленная экология |
| Культурология |
| Социальная психология |
| Психология и педагогика |
| Правоведение |
| Криптографические методы защиты информации |
| Мировая экономика |

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

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

| |
|---|
| Исследование операций и теории игр |
| Теория графов и ее приложения |
| ОПК-3 «способность применять языки, системы и инструментальные средства программирования в профессиональной деятельности» |
| Информатика |
| Основы программирования |
| Технологии и методы программирования |
| Криптографические методы защиты информации |
| Программно-аппаратные средства обеспечения информационной безопасности |
| Методы и средства проектирования информационных систем |
| Языки программирования |
| Научно-исследовательская работа |
| ОПК-4 «способность понимать значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах» |
| Промышленная экология |
| Информатика |
| Экология |
| Основы программирования |
| Информационные технологии |
| Основы информационной безопасности |
| Технологии и методы программирования |
| Безопасность жизнедеятельности |
| Теория информации |
| Теория информационной безопасности |
| Моделирование систем |
| Техническая защита информации |
| Языки программирования |
| Защита информации в распределенных информационных системах |
| Научно-исследовательская работа |
| Информационная безопасность распределенных информационных систем |
| Технология построения защищенных распределенных приложений |
| ОПК-5 «способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами» |
| Инженерная графика |
| Криптографические методы защиты информации |
| Научно-исследовательская работа |
| Научно-технический семинар |
| ОПК-6 «способность применять нормативные правовые акты в профессиональной деятельности» |
| Стандарты информационной безопасности |
| Метрология |

| |
|---|
| Микропроцессорная техника |
| Теория информационной безопасности |
| Организационное и правовое обеспечение информационной безопасности |
| ОПК-7 «способность применять приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций» |
| Промышленная экология |
| Экология |
| Безопасность жизнедеятельности |
| ОПК-8 «способность к освоению новых образцов программных, технических средств<br>и информационных технологий» |
| Основы радиотехники |
| Архитектура информационных систем |
| Электроника и схемотехника |
| Организация ЭВМ и вычислительных систем |
| Программно-аппаратные средства обеспечения информационной безопасности |
| Сети и системы передачи информации |
| Моделирование систем |
| Теория кодирования |
| Безопасность систем баз данных |
| Методы и средства проектирования информационных систем |
| Разработка и эксплуатация защищенных автоматизированных систем |
| Надежность информационных систем |
| Проектирование безопасных информационных систем |
| Разработка мобильных приложений |
| Технология построения защищенных распределенных приложений |
| ПК-1 «способность осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке» |
| Основы программирования |
| Теория графов и ее приложения |
| Научно-технический семинар |
| ПК-2 «способность создавать и исследовать модели автоматизированных систем» |
| Устройства и системы беспроводной связи |
| Методы проектирования защищенных распределенных информационных систем |
| ПК-3 «способность проводить анализ защищенности автоматизированных систем» |
| Распределенные сети хранения данных |
| Распределенные информационные системы |
| Информационная безопасность распределенных информационных систем |
| Методы проектирования защищенных распределенных информационных систем |
| ПК-4 «способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы» |
| Технологии защиты от скрытой передачи данных |
| Защита от вредоносных программ |

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

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

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

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

| |
|---|
| разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах» |
| Методы проектирования защищенных распределенных информационных систем |
| ПСК-7.3 «способность проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем» |
| Исследование операций и теории игр |
| Технология построения защищенных распределенных приложений |
| ПСК-7.4 «способность проводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах» |
| Теория графов и ее приложения |
| Информационная безопасность распределенных информационных систем |
| ПСК-7.5 «способность координировать деятельность подразделений и специалистов по защите информации на предприятии, в учреждении, организации» |
| Информационная безопасность распределенных информационных систем |

4.1.3. Методические рекомендации обучающимся по подготовке к ГЭ.

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).

## 5 ТРЕБОВАНИЯ К ВЫПУСКНОЙ(ЫМ) КВАЛИФИКАЦИОННОЙ(ЫМ) РАБОТЕ(АМ) И ПОРЯДКУ ИХ ВЫПОЛНЕНИЯ

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

Дипломная работа может иметь исследовательский характер или представлять собой решение практической задачи одной из актуальных проблем специальности в области защиты информации и обеспечения информационной безопасности выбранного объекта.

Объектами дипломной работы могут быть методы и средства защиты информации, методы анализа уязвимости информации объектов, методы обоснования надежности (достаточности) выбранных мер защиты информации, методы экономической оценки эффективности предлагаемых защитных мероприятий и т.д.

В соответствие с требованиями Федерального Государственного образовательного стандарта дипломная работа по специальности 10.05.05 «Безопасность информационных

технологий в правоохранительной сфере» представляет собой законченную разработку в профессиональной области, в которой:8

− сформулирована актуальность и место решаемой задачи по защите информации в предметной области;

− проанализированы литература и информация по организации и используемых технологий по защите информации в данной области или в смежных предметных областях;

− определены и конкретно описаны выбранные дипломантом объемы, методы и средства решаемой задачи, иллюстрируемые данными и нормативными документами, используемые при реализации поставленной задачи по защите информации в предметной области;

− проанализированы предлагаемые пути, способы решения поставленных задач, а также оценивается экономическая, техническая и (или) социальная эффективность их внедрения в реальную информационную среду применения.

В соответствии с перечисленными требованиями в общем случае в дипломной работе студент-дипломник должен:

− обосновать актуальность и значимость решаемой задачи по обеспечению защиты выбранного информационного объекта;

− выполнить анализ литературы по вопросам выбранной темы работы; − сформулировать сущность задачи по защите информации;

− провести аудит информационной безопасности защищаемого объекта;

− выявить возможные каналы утечки исследуемого объекта информатизации;

− разработать систему защиты информации (СЗИ) согласно нормативно-методических документов;

− обосновать выбор средств защиты информации;

− разработать мероприятия по внедрению СЗИ на объекте и предложить методику применения выбранных средств защиты;

− выполнить экономические расчеты (расчет экономической эффективности внедрения результатов работы, или расчет каких-либо других экономических показателей), характеризующих целесообразность внедрения предлагаемых мероприятий по защите информации.

Общими требованиями к дипломной работе являются:

− целевая направленность;

− четкость построения;

− логическая последовательность изложения материала;

− убедительность аргументаций;

− краткость и точность формулировок;

− конкретность изложения результатов работы;

− доказательность выводов и обоснованность рекомендаций;

− грамотное оформление.

Структурными элементами дипломной работы являются:

1. Титульный лист.
2. План и график выполнения дипломной работы.
3. Содержание.
4. Введение.
5. Основная часть (главы, параграфы, пункты).
6. Заключение.
7. Список использованных источников.
8. Приложения.
9. Презентация, демонстрационный материал

Дипломная работа может иметь исследовательский характер или представлять собой решение практической задачи одной из актуальных проблем специальности в

области защиты информации и обеспечения информационной безопасности выбранного объекта.

Объектами дипломной работы могут быть методы и средства защиты информации, методы анализа уязвимости информации объектов, методы обоснования надежности (достаточности) выбранных мер защиты информации, методы экономической оценки эффективности предлагаемых защитных мероприятий и т.д.

**Содержание** включает в себя наименование всех разделов (глав) и пунктов (параграфов), имеющих наименования, с указанием страниц.

**Во введении** обосновываются ***актуальность*** выбранной темы, цель и содержание поставленных задач, формулируются объект и предмет исследования, указывается избранный метод (или методы) исследования, сообщается, в чем заключается теоретическая значимость и прикладная ценность полученных результатов, а также отмечаются положения, которые выносятся на защиту. Если студент принимал участие в семинарах и конференциях, на которых выступал с докладами, то необходимо указать конференции и количество опубликованных работ, если такие имеются. Рекомендуется указать объем и структуру ВКР, а именно, количество машинописных страниц, рисунков, таблиц, количество использованных источников и количество приложений. Объем введения – не более трех страниц текста.

**Основная часть ВКР** состоит из глав (главы), которые могут подразделяться на пункты (параграфы). В общем случае основная часть ВКР может содержать 3-4 главы, структура (деление на параграфы) и содержание которых зависит от темы и анализируемого материала.

Содержание глав основной части должно точно соответствовать их наименованиям, теме работы и полностью её раскрывать. Материал должен излагаться сжато, логично и аргументировано. Примерное содержание отдельных глав основной части ВКР.

*Глава 1. Аналитическая часть.* Основная цель первой главы – рассмотрение существующего состояния предметной области, характеристика объекта защиты, анализ существующих методов и средств, применяемых для контроля и защиты информации и обоснование предложений по устранению выявленных недостатков и т.д. В главе выполняется постановка задачи выпускной квалификационной работы.

Материал первой главы (Аналитическая часть) рекомендуется структурировать следующим образом.

1.1. Технико-экономическая характеристика предметной области (объекта защиты или исследования).

1.2. Нормативно-методическая база в области защиты информации предметной области.

1.3. Описание модели вероятного злоумышленника объекта защиты (анализ и систематизация уязвимостей объекта защиты, ранжирование угроз, построении граф-моделей проникновения и т.д.).

1.4. Анализ методик решения аналогичных задач.

1.5. Маркетинговые исследования в области технических и программных средств защиты информации в предметной области.

Аналитическая часть должна заканчиваться выводами по рассмотренным вопросам с обоснованием главных направлений проектных решений. Объем аналитической части может составлять 20-25 страниц.

*Глава 2. Проектная часть.* Вторая глава посвящена вопросам проектирования. Задачей проектной части ВКР является реализация и описание предложенных студентом разработок в рамках выбранной темы и с учетом специфики конкретного объекта и аспектов исследования, подходов, методов и средств решения конкретных задач.

В рамках разработок могут включаться задачи совершенствования (улучшения) существующих систем обеспечения безопасности выбранного объекта. При этом на

основе принятых проектных предложений следует определить и указать их конкретную конфигурацию, схему применения обеспечивающих безопасность объекта.

Проектная часть должна содержать материал, соответствующий исключительно конкретным особенностям объекта и задачам разработки. В соответствии с поставленными задачами материал главы может быть структурирован следующим образом:

2.1. Описание модели безопасности объекта.

2.2. Алгоритмы решения поставленных задач по защите выбранного объекта в области исследования (вербальная форма, математическая, блок-схемы и программные модули с описанием предлагаемого алгоритма защиты).

2.3. Информационные модели защищаемого информационного ресурса.

2.4. Комплексы инженерно-технических средств по обеспечению информационной безопасности объекта.

2.5. Структуры аппаратных и программно-аппаратных защитных средств.

Проектную часть желательно закончить кратким перечнем основных предложенных в работе проектных решений. Примерный объем проектной части составляет 30-40 страниц.

*Глава 3. Оценка экономической эффективности (правовая оценка)* предлагаемой системы информационной безопасности.

В выпускной квалификационной работе должна быть выполнена оценка эффективности внедрения на предприятии проектных предложений по обеспечению информационной безопасности объектов защиты. Возможны различные подходы к ее определению:

1. Сравнение вариантов существовавшей системы безопасности объекта (ов) защиты, разработанной студентом, и с расстановкой акцентов на ее преимуществах.

2. Расчет количественных характеристик экономической эффективности, определяемой из соотношений между гипотетическими доходами, измеряемыми возможными потерями из-за отсутствия надежной системы безопасности на объектах защиты, и произведенными затратами на внедрение предложенной системы.

3. Обоснование внедрения в практику разработанных методик, моделей, лабораторных работ, тренажеров по моделированию направлений защиты объекта защиты, комплектов документации объекта защиты для службы (отдела) защиты информации.

Кроме этого, можно оценить улучшение качественных характеристик процесса функционирования предприятия и влияние предлагаемых разработок на эффективность его деятельности. Примерный объем этой части ВКР составляет 10-15 страниц.

В **Заключении** необходимо показать особенность и оригинальность работы, применение новых подходов при решении поставленных задач и описать мероприятия по реализации проектных решений, разработанных в выпускной квалификационной работе, привести рекомендации по использованию результатов работе, а также отразить основные выводы и рекомендации по результатам выполненной вкр.

Выводы желательно нумеровать или выделять маркерами, их число не должно превышать 5-6. Каждый вывод должен начинаться с новой строки и состоять из одного или двух коротких предложений. Объем заключения должен быть не более двух-трех страниц.

5.2. Дополнительные компоненты ВКР, определяемые выпускающей кафедрой.

Программный код разработанного приложения приводится в приложении к пояснительной записке.

5.3. Наличие/отсутствие реферата в структуре ВКР.

Реферат не предусмотрен.

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

Структура иллюстративно–графического материала повторяет структуру пояснительной записки к ВКР.

Графический материал – технологические схемы, генеральные планы, диаграммы, таблицы и другой материал, отвечающий требованиям единой системы конструкторской документации (ЕСКД).

Иллюстративный материал – рисунки, фотографии, презентации, разработанные студентом-дипломником для демонстрации в процессе защиты работы.

Объем графического или иллюстративного материала должен составлять для дипломной работы не менее 8 и не более 16 листов (слайдов). При выполнении чертежа на двух и более листах (слайдах) их надлежит снабжать одной основной надписью. В этом случае выполненный графический материал учитывается как один лист.

Графический материал по размерам и исполнению должен свободно просматриваться с расстояния 3–3,5 м, что соответствует шрифтам при электронном наборе макетов плакатов формата А4 с последующей распечаткой в формате А1 для заголовка – 24 пт, подрисуночных подписей, заголовков таблиц – 18 пт, обозначений на рисунках и текста в таблицах – 16 пт.

Диаграммы, графики, рисунки дипломных работ должны быть выполнены с помощью компьютерной графики.

Иллюстративный (графический) материал необходимо размещать на стандартных листах, выполнять в соответствии с правилами оформления иллюстраций в тексте пояснительной записки и снабжать заголовком и основной надписью.

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

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

– актуальности темы;

– полноты решения поставленных задач;

– степени самостоятельности и инициативности студента;

– умения студента пользоваться специальной литературой;

– способности студента к исследовательской работе;

– возможности использования полученных результатов на практике;

– возможности присвоения выпускнику соответствующей квалификации.

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

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

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

– актуальность темы работы;

– степень соответствия работы заданию;

– соответствие содержания пояснительной записки требованиям стандарта;

– наличие критического обзора литературы, его полнота и последовательность анализа;

– полнота описания методики расчетов или проведенных исследований и оценка достоверности полученных результатов;

– наличие аргументированных выводов по результатам работы;

– практическая значимость работы;

– недостатки и слабые стороны работы;

– замечания по оформлению пояснительной записки к дипломной работе и стилю изложения материала;

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

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

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

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

После публичной защиты ВКР проводится закрытое совещание членов ГЭК, на котором обсуждаются результаты защиты, и определяется общая оценка подготовки и защиты ВКР каждого студента. Результаты защиты объявляются председателем ГЭК в день защиты после закрытого заседания комиссии и оформления соответствующих протоколов. Вместе с объявлением оценок председатель ГЭК зачитывает решение комиссии о присвоении студентам-выпускникам соответствующей квалификации.

Критерии оценки.

Оценка «отлично» выставляется при условии выполнения следующих требований:

– представленная дипломная работа соответствует всем установленным критериям:

– тематика дипломной работы соответствует содержанию одного или нескольких профессиональных модулей;

– содержание дипломной работы соответствует заявленной теме, тема раскрыта полностью;

– обзор литературы и источников отличается полнотой и обстоятельностью, соответствует выбранной теме;

– экспериментальная часть характеризуется актуальностью, оригинальностью, новизной, ценностью поставленных задач, поставленные задачи сформулированы четко и ясно и соответствуют теме, исследование по поставленным задачам проведено в полном объеме, материал экспериментальной части приведен в наглядной форме, продемонстрирован достаточный уровень практических умений и результатов приобретенного практического опыта;

– оформление соответствует установленным нормам и требованиям;

– доклад студента по всем показателям демонстрирует в полном объеме овладение общими и профессиональными компетенциями, предусмотренными ФГОС, учебными программами дисциплин и профессиональных модулей;

– студент ориентируется во всех дополнительных вопросах.

Оценка «хорошо» выставляется при условии выполнения следующих требований:

– тематика дипломной работы соответствует содержанию одного или нескольких профессиональных модулей;

– представленная дипломная работа соответствует всем или почти всем установленным критериям на хорошем уровне (не допускается несоответствие содержания заявленной тематике и требованиям по оформлению);

– доклад студента показывает хорошее усвоение теоретического материала, овладение общими и профессиональными компетенциями, предусмотренными ФГОС, учебными программами дисциплин и профессиональных модулей;

– студент готов к конкретным видам профессиональной деятельности техника по защите информации;

– студент ориентируется во всех дополнительных вопросах, при этом возможны некоторые неточности.

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

– тематика дипломной работы соответствует содержанию одного или нескольких профессиональных модулей;

– представленная дипломная работа удовлетворяет всем требованиям по оформлению, соответствует заявленной теме, однако имеются существенные недостатки по её содержанию;

– студент показывает неполное усвоение теоретического материала, овладение общими и профессиональными компетенциями, предусмотренными ФГОС, учебными программами дисциплин и профессиональных модулей, отвечает не на все дополнительные вопросы;

– приложения удовлетворительного качества или не представлены.

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

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

Подготовка ВКР предполагает последовательное выполнение следующих этапов:

– подбор и первоначальное ознакомление с учебной и научной литературой, материалами специальной периодической печати, нормативно-законодательными и инструктивными документами и другими источниками информации по выбранной теме;

– составление предварительного плана дипломной работы (совместно с руководителем);

– прохождение преддипломной практики;

– изучение отобранных источников информации и фактических материалов организации;

– обработка фактического материала;

– участие в студенческой научно-технической конференции с целью апробации основных подходов к совершенствованию учетно-аналитического и контрольного процессов в конкретной организации, сформулированных по результатам преддипломной практики;

– составление окончательного плана ВКР и задания на дипломное проектирование (совместно с руководителем);

– написание и оформление ВКР, разработка иллюстративного (графического) материала в соответствии с календарным графиком;

– поэтапное (в соответствии с календарным графиком) представление результатов дипломного исследования руководителю дипломной работы, консультантам по специальным разделам (технология производства, охрана труда и безопасность жизнедеятельности), в рабочую комиссию по контролю за ходом дипломного проектирования;

– поэтапная (в соответствии с календарным графиком) доработка ВКР по замечаниям руководителя, консультантов, рабочей комиссии;

– представление готовой работы на нормоконтроль;

– передача ВКР на отзыв руководителю и ознакомление с отзывом;

– получение в рабочей комиссии рекомендации к защите ВКР;

– представление ВКР заведующему кафедры (вместе с отзывом руководителя и рекомендацией рабочей комиссии к защите) для заключения о возможности допуска ее к защите;

– передача ВКР на рецензию и ознакомление с замечаниями рецензента;

– подготовка доклада, иллюстративного материала или презентации к защите ВКР.

В ходе выполнения ВКР студент должен разобраться в теоретических аспектах избранной темы, в рамках темы исследования ознакомиться с нормативно-законодательными документами и инструктивными материалами вышестоящих органов, международными стандартами защиты информации и зарубежным опытом, проанализировать собранный практический материал, разработать и научно обосновать предложения по

совершенствованию системы информационной безопасности в организации. Для решения данных задач необходимо подобрать литературные и другие источники информации, собрать и обработать практический материал по исследуемому предприятию.

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

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

## 7 ПЕРЕЧЕНЬ РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ ДЛЯ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

### 7.1. Основная литература

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

Таблица 3 – Перечень основной литературы

| Шифр/URL адрес | Библиографическая ссылка | Количество экземпляров в библиотеке (кроме электронных экземпляров) |
|---|---|---|
| 004<br>И 74 | Информационный менеджмент [Текст] : учебник / Н. М. Абдикеев [и др.] ; ред. Н. М. Абдикеев. - М. : ИНФРА-М, 2012. - 400 с. | 50 |
| 681.3<br>М 48 | Мельников, В. П. Информационная безопасность [Текст] : учебное пособие для СПО / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; ред. С. А. Клейменов. - 7-е изд., стер. - М. : Академия, 2012. - 332 с. | 40 |
| 004<br>Ф 34 | Федотова, Е. Л. Информационные технологии и системы [Текст] : учебное пособие / Е. Л. Федотова. - М. : ФОРУМ : ИНФРА-М, 2012. - 352 с. | 50 |
| 355/359<br>О-93 | Оценка устойчивости функционирования объектов экономики [Текст] : методические указания к практическим занятиям / С.-Петерб. гос. ун-т аэрокосм. приборостроения ; Сост. А. В. Матвеев, Ю. В. Симагин. - СПб. : Изд-во ГУАП, 2013. - 44 с. | 200 |
| Х<br>Т 69 | Трифонова, Юлия Викторовна. Организация обработки персональных данных в соответствии с законодательством | 60 |

| | | |
|---|---|---|
| | РФ [Текст] : учебное пособие / Ю. В. Трифонова ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - СПб. : Изд-во ГУАП, 2013. - 99 с. | |
| 004<br>М 87 | Мошак, Николай Николаевич (проф.). Защищенные инфотелекоммуникации. Анализ и синтез [Текст] : монография / Н. Н. Мошак ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - СПб. : Изд-во ГУАП, 2014. - 197 с. | 40 |
| 004<br>М 87 | Мошак, Николай Николаевич (проф.). Организация безопасного доступа к информационным ресурсам [Текст] : учебное пособие / Н. Н. Мошак, Т. М. Татарникова ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - СПб. : Изд-во ГУАП, 2014. - 121 с. | 40 |

7.2. Дополнительная литература

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

Таблица 4 – Перечень дополнительной литературы

| Шифр/URL адрес | Библиографическая ссылка | Количество экземпляров в библиотеке (кроме электронных экземпляров) |
|---|---|---|
| 004<br>И 74 | Информационные системы и технологии в экономике и управлении [Электронный ресурс] : учебник / С.-Петерб. гос. ун-т экономики и финансов ; ред. В. В. Трофимов. - 3-е изд. перераб. и доп. - Электрон. текстовые дан. - М. : Юрайт, 2012. | 1 |
| Х<br>С 50 | Смирнов, А. А. Обеспечение информационной безопасности в условиях виртуализации общества : Опыт Европейского Союза [Текст] / А. А. Смирнов. - М. : ЮНИТИ-ДАНА : Закон и право, 2012. - 159 с. | 2 |
| 004(075)<br>А 91 | Астахова, А. В. Информационные системы в экономике и защита информации на предприятиях - участниках ВЭД [Текст] : учебное пособие / А. В. Астахова. - СПб. : Троицкий мост, 2014. - 216 с. : рис., табл. - Библиогр.: с. 210 - 214 | 5 |
| 004<br>М 48 | Мельников, В. П. Защита информации [Текст] : учебник / В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе ; ред. В. П. Мельников. - М. : Академия, 2014. - 304 с. | 10 |
| 004<br>О-54 | Олифер, В. Г. Безопасность компьютерных сетей [Текст] : [учебное пособие] / В. Г. Олифер, Н. А. Олифер. - М. : Горячая линия - Телеком, 2014. - 644 с. | 10 |

## 8 РЕСУРСЫ ИНФОРМАЦИОННО–ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ»

Перечень ресурсов информационно–телекоммуникационной сети «Интернет»,

необходимых при подготовке к ГИА, представлен в таблице 5.

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

| URL адрес | Наименование |
|---|---|
| www.intuit.ru | Национальный Открытый Университет "ИНТУИТ" |

## 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 | Лекционная аудитория | |
| 2 | Компьютерный класс | |

## 10 ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

10.1. Фонд оценочных средств для проведения ГЭ.

10.1.1. Состав фонда оценочных средств приведен в таблице 7.

Таблица 7 – Состав фонда оценочных средств для проведения ГЭ

| Форма проведения ГЭ | Перечень оценочных средств |
|---|---|
| Письменная | Список вопросов к экзамену<br>Задачи |

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

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

Описание показателей для оценки компетенций для ГЭ:

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

– умение справляться с задачами;

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

– уровень правильности обоснования принятых решений при выполнении практических задач.

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

В качестве критериев оценки уровня сформированности (освоения) у студентов компетенций при проведении ГЭ в формах «устная» и «письменная» применяется 4–балльная шкала, а при проведении ГЭ с применением средств электронного обучения применяется 100–балльная шкала (таблица 8).

Таблица 8 –Критерии оценки уровня сформированности компетенций

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

| | | |
|---|---|---|
| | | – не формулирует выводов и обобщений. |

10.1.4. Типовые контрольные задания или иные материалы

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

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

| № п/п | Список вопросов для ГЭ, проводимого в письменной/устной форме | Компетенции |
|---|---|---|
| | Помехоустойчивое кодирование.<br>Потери информации в РИС.<br>Пассивные и активные угрозы безопасности информации в РИС.<br>Меры, предпринимаемые для обеспечения безопасности информации в сосредоточенных ИС | ОК-1 |
| | Необходимость поддержки механизмов аутентификации и разграничения доступа удаленных процессов к ресурсам объекта,<br>Специализированные коммуникационные компьютерные системы. Концентраторы, коммуникационные модули (серверы), шлюзы и мосты Виды шифрования в ИС: линейное и абонентское шифрование.<br>Центр управления сетью. | ОК-2 |
| | Организация процессов обработки данных в БД. Индексирование таблиц. Связывание таблиц.<br>Постреляционная и многомерная модель данных.<br>Реляционная алгебра (объединение, пересечение, вычитание, произведение, выборка).<br>Реляционная алгебра (проекция, деление, соединение).<br>Язык SQL. | ОК-3 |
| | Коммутационная подсистема РИС<br>Подсистемы РИС<br>Особенности защиты информации в РИС<br>Корпоративные и общедоступные РИС.<br>Построение системы защиты информации в РИС.<br>Особенности защиты информации от непреднамеренных угроз в РИС. | ОК-4 |
| | Механизмы для защиты информации при передаче ее по каналам связи<br>Механизмы для защиты информации для защиты от несанкционированного воздействия<br>Методы и средства, обеспечивающие безопасность информации в защищенной вычислительной сети<br>Обеспечение безопасности информации в специализированных коммуникационных ИС | ОК-5 |
| | Базы данных. СУБД. Классификация.<br>Типология БД. Документальные БД. Фактографические БД. | ОК-6 |

| | | |
|---|---|---|
| | Типология БД. Гипертекстовые и мультимедийные БД. Объектно-ориентированные БД.<br>Типология БД. Распределенные БД. Коммерческие БД.<br>Иерархическая и сетевая модели данных.<br>Элементы реляционной модели данных.<br>Реляционное исчисление. Организация процессов обработки данных в БД. Ограничения целостности. | |
| | Проблемы проектирования реляционных БД.<br>Принципы построения БД. Нормальные формы: 1НФ, 2НФ, 3НФ.<br>Принципы построения БД. Метод «Сущность-связь».<br>Пример разработки ER-модели.<br>Хранение отношений. Организация индексов.<br>Транзакции. Сериализация транзакций.<br>Жизненный цикл БД. Модели жизненного цикла ПО.<br>Модели структурного проектирования. Метод структурного анализа и проектирования. | ОК-7 |
| | Общие задачи и главные компоненты глобальных сетей – WAN<br>IP адресация, две составные части адреса, подсети.<br>ARP- запросы, таблицы, ответы, RARP – сервера, запросы и ответы.<br>Характеристики топологий шина, звезда, расширенная звезда. Преимущества и недостатки.<br>Стандарты, используемые при проектировании LAN. Кабели и их характеристики.<br>Уровень приложений, представлений, сеансовый и транспортный уровни модели OSI.<br>Функции уровня приложений протокола TCP/IP.<br>Функции транспортного уровня протокола TCP/IP. | ОК-8 |
| | Протоколы ICMP, ARP, RARP, UTP<br>Маршрутизация с использованием вектора расстояний и с учетом состояния канала связи, гибридная маршрутизация.<br>Команды и процесс настройки маршрутизатора. Пользовательский и привилегированный режимы.<br>Компоненты участвующие в конфигурировании маршрутизатора. Тестирование с помощью команд show, telnet, ping, trace, shoew ip route, show interface serial.<br>Конфигурирование маршрутизатора, начальная установка глобальных параметров и параметров интерфейсов. | ОК-9 |
| | Проблема создания и сжатия больших информационных массивов, информационных хранилищ и складов данных. Сжатие без потерь в реляционных СУБД.<br>Защита информации в БД<br>Функции каждого из уровней эталонной модели OSI<br>Процесс инкапсуляции и взаимодействия между уровнями эталонной модели OSI.<br>Программные и аппаратные особенности различных способов организации локальных сетей.<br>Описание и назначение сетевого адаптора и MAC адреса.<br>Описание и назначение и функции сетевых устройств повторители, хабы, мосты, свичи, маршрутизаторы. | ОПК-1 |
| | Какие мероприятия необходимо провести для обеспечения защиты информации при проведении переговоров и совещаний?<br>Что следует сделать для обеспечения безопасности конфиденциальной информации в рекламно-выставочных материалах? | ОПК-2 |

| | | |
|---|---|---|
| | Как осуществляется защита информации при работе с посетителями?<br>Что необходимо сделать для организации защиты персональных данных в кадровой службе?<br>Ставится ли гриф ограничения на личные дела сотрудников предприятия?<br>Сформулируйте правила, которые следует соблюдать при работе с конфиденциальными документами. | |
| | В какой момент времени работнику следует подписать обязательства о неразглашении конфиденциальных сведений предприятия?<br>Какие пункты, оговаривающие процедуру защиты информации предприятия, можно включить в трудовой договор?<br>В чем заключаются особенности увольнения сотрудников, владеющих конфиденциальной информацией предприятия?<br>Что представляет собой процесс лицензирования деятельности по защите информации в РФ? | ОПК-3 |
| | Понятие уязвимости информации<br>Методологическая основа раскрытия сущности и определения понятия защиты информации.<br>Понятие носитель защищаемой информации". Соотношение между носителем и источником информации.<br>Виды отображения информации в носителях<br>Современные подходы к понятию угрозы защищаемой информации<br>Понятие угрозы защищаемой информации.<br>Понятие объекта защиты. | ОПК-4 |
| | Какие задачи решает антикризисная группа?<br>Назовите основные задачи, решаемые службой безопасности предприятия.<br>Какими нормативными документами руководствуется служба безопасности в своей деятельности?<br>Какие функции выполняет служба безопасности на предприятии?<br>Назовите, какие виды пропускных документов применяются при организации внутриобъектового режима предприятия? | ОПК-5 |
| | Дайте характеристику основным направлениям информационно-аналитической работы.<br>Что показывают результаты информационно – аналитической работы?<br>На основе каких данных выполняется поиск каналов НСД к ценной информации?<br>Изложите порядок проведения информационно-аналитической работы. | ОПК-6 |
| | Модель OSI.<br>Задачи обеспечения безопасности информации в сети на различных уровнях.<br>Проблемы защиты информации в РИС<br>Защита информации в каналах связи<br>Комплекс методов и средств защиты, позволяющих блокировать возможные угрозы безопасности информации. | ОПК-7 |
| | Безусловно стойкие и вычислительно стойкие шифры.<br>Псевдослучайные последовательности (ПСП). Характеристики генераторов ПСП (ПСГ). Требования к криптографическим ПСП. Примеры ПСГ и криптографических ПСГ.<br>Поточные шифры. Общая схема поточного шифра. Синхронные и самосинхронизирующиеся шифры.<br>Регистры сдвига с обратной линейной связью (РСЛОС).<br>ПСГ на основе РСЛОС.<br>Шифр А5. | ОПК-8 |

| | | |
|---|---|---|
| | На каких принципах организуется защита информации, обрабатываемой в информационных системах?<br>Для чего необходимо проводить информационно-аналитическую работу?<br>Какие задачи необходимо выполнить при информационно-аналитической работы?<br>Какое подразделение службы безопасности предприятия занимается информационно – аналитической работой? | ПК-1 |
| | Средства защиты информации специализированной ИС администратора сети как от непреднамеренных, так и от преднамеренных угроз.<br>Защита процедур со средств, связанных с хранением и работой с ключами.<br>Механизмы, блокирующие возможность работы с информационной частью сообщений, которые не предназначаются администратору<br>Управление передачей сообщений по определенным протоколам Международные стандарты взаимодействия удаленных элементов сети: протокол TCP/IP и протокол X.25. | ПК-2 |
| | Подходы к криптоанализу блочных шифров. Дифференциальный криптоанализ. Линейный криптоанализ.<br>Режимы шифрования.<br>Многократное шифрование. Композиция блочных шифров.<br>Совершенные шифры. Пример совершенного шифра.<br>Энтропийные характеристики шифров. Идеальные шифры.<br>Избыточность языка.<br>Оценка числа ложных ключей и расстояние единственности. | ПК-3 |
| | Состав объектов хранения письменных и видовых носителей информации, подлежащих защите.<br>Другие объекты защиты информации. Виды и способы дестабилизирующего воздействия на объекты защиты.<br>Виды защиты информации, сферы их действия<br>Классификация методов защиты информации | ПК-4 |
| | Перечистите основные виды аутентификации.<br>В чем заключается повышение надежности и отказоустойчивости информационных систем?<br>Какую роль играет подготовленность персонала в построении системы защиты информации?<br>Какие методы и средства используются для организации противодействия традиционным методам шпионажа и диверсий?<br>Раскройте особенность построения защиты от несанкционированного доступа<br>Какие методы защиты информации относятся к криптографическим? | ПК-5 |
| | Какое значение имеют составляющие информационной безопасности для субъектов информационных отношений?<br>Каковы интересы РФ в информационной сфере?<br>Определите источники угроз информационной безопасности РФ и постройте их классификацию.<br>Перечислите основные методы обеспечения информационной безопасности РФ.<br>Какие основные проблемы международного сотрудничества | ПК-6 |

| | | |
|---|---|---|
| | стоят на повестке дня сегодня?<br>Перечислите основные документы в области международной информационной безопасности.<br>Каково, на ваш взгляд, положение дел в области МИБ сегодня?<br>Проанализируйте различные определения понятия «защита информации» и «информационная безопасность». | |
| | Дайте определение понятию защита информации.<br>Что понимается под термином безопасность информации?<br>Что включает в себя защита информации?<br>Какие цели преследует защита информации?<br>Какое место занимается защита информации в информационной безопасности?<br>Какие уровни задействованы в обеспечении информационной безопасности?<br>Что представляет собой политика безопасности организации? | ПК-7 |
| | Что входит в анализ рисков?<br>Что представляет собой программа безопасности организации?<br>Определите предмет защиты информации.<br>Сформулируйте основные свойства информации.<br>Дайте определение конфиденциальной информации.<br>Перечислите уровни секретности государственной тайны.<br>Раскройте сущность основных подходов к измерению количества информации.<br>Раскройте сущность информации как объекта права собственности. 7. Раскройте сущность объекта защиты. | ПК-8 |
| | Составьте классификацию угроз информационной безопасности.<br>Раскройте основные группы классификации.<br>На основании чего строится модель нарушителя информационной безопасности?<br>Сформулируйте основные принципы построения системы защиты информации.<br>Перечислите основные модели защиты информации и их особенности.<br>В чем заключается сущность методов защиты от случайных угроз?<br>Дайте определение понятиям идентификации и аутентификации. | ПК-9 |
| | Шифрование на абонентском уровне.<br>Линейное шифрование.<br>Процедуры взаимного подтверждения подлинности абонентов или процессов<br>Особенности защиты информации в распределенных базах данных<br>Базы данных как надежное хранилище структурированных данных<br>Проблемы защиты информации от преднамеренных угроз, поддержания актуальности и непротиворечивости данных.<br>Встраивание механизмов защиты в СУБД или использование их в виде отдельных компонент.<br>Решение задач разграничения доступа, поддержания физической целостности и логической сохранности данных. | ПК-10 |

| | | |
|---|---|---|
| | Использование отказоустойчивых устройств, построенных по технологии RAID.<br>Шифрование с помощью единого ключа, или индивидуальных ключей пользователей.<br>Режимы работы с зашифрованными базами данных.<br>Методы противодействия угрозам информации в базах данных<br>Основные понятия и определения криптографии. | ПК-11 |
| | Для чего организуют внутриобъектовый режим на предприятии?<br>Как оценивается эффективность системы защиты предприятия?<br>Назовите, какие существуют виды охраны объектов?<br>Для чего на объекте организуется многорубежная защита? Какими достоинствами обладает такой вид организации защиты объекта?<br>Что такое коммерческая тайна?<br>Какие мероприятия предусматривает защита коммерческой тайны?<br>Что относится к средствам инженерно – технической защиты информации?<br>Что понимается под разглашением коммерческой тайны? | ПК-12 |
| | Какие бывают виды аналитических отчетов?<br>Что должен включать аналитический отчет?<br>Назовите современные методы аналитических исследований.<br>Назовите основные этапы проведения совещания.<br>Кто дает разрешение на проведение конфиденциального совещания?<br>Что не разрешается делать участникам конфиденциального совещания?<br>Кто несет ответственность за обеспечение безопасности ценной информации при проведении конфиденциального совещания? | ПК-13 |
| | Назовите основные этапы профотбора сотрудников для работы на коммерческом предприятии.<br>Назовите группы людей, от которых могут исходить угрозы информационным ресурсам предприятия.<br>Приведите примеры тестовых методик, применяемых при отборе сотрудников.<br>Какова структура заключительного собеседования? | ПК-14 |
| | На каких принципах основана процедура проведения сертификации средств защиты информации?<br>Сущность информационной безопасности. Объекты информационной безопасности<br>Связь информационной безопасности с информатизацией общества<br>Значение информационной, безопасности для субъектов информационных<br>Место информационной, безопасности, в системе национальной безопасности.<br>Существующие подходы к содержательной части понятия "защита информации" и способы реализации содержательной части | ПК-15 |
| | История криптографии. Основные этапы становления науки криптографии.<br>Классификация шифров замены. Шифр Цезаря. Шифр простой замены. Шифр Плейфера. Полибианский квадрат. Шифр Хилла. Шифр Виженера. Частотный анализ. Тест Казиски.<br>Классификация шифров перестановки. Примеры шифров перестановки и их криптоанализ.<br>Шифры гаммирования. Шифр Вернама. Подходы к его криптоанализу. | ПК-16 |
| | Нелинейные регистры сдвига.<br>Шифр RC4. | ПК-17 |

| | | |
|---|---|---|
| | Теория имитостойкости Симмонса. Имитация и подмена сообщения. Характеристики имитостойкости. Совершенная имитостойкость.<br>Коды аутентификации сообщений.<br>Защитные контрольные суммы.<br>Криптографические хэш-функции и требования к ним.<br>Подходы к проектированию хэш-функций.<br>Хэш-функции на основе блочного шифра.<br>Ключевые хэш-функции.<br>Понятие односторонней функции и односторонней функции с "лазейкой". Проблемы факторизации целых чисел и логарифмирования в конечных полях.<br>Криптосистема Диффи-Хэллмана. Пример.<br>Криптосистема RSA. Пример. | |
| | Криптосистема Эль-Гамаля. Пример.<br>Криптосистема Рабина. Пример.<br>Криптосистема Гольдвассер-Микали. Пример.<br>Криптосистема Блюма-Гольдвассер. Пример.<br>Рюкзачные шифры. Криптосистема Меркла-Хэллмана.<br>Понятие электронной цифровой подписи и требования к ней. Атаки и угрозы схемам ЭЦП. | ПК-18 |
| | Проблема дискретного логарифмирования на эллиптической кривой. Переход от шифра (ЭЦП) в Zp к шифру (ЭЦП) на эллиптической кривой.<br>Шифр Эль-Гамаля на эллиптической кривой.<br>Стандарты ЭЦП на эллиптической кривой: ГОСТ Р 34.10-2001, ECDSA.<br>Перечислите виды угроз информационной безопасности РФ.<br>Что является источниками угроз информационной безопасности РФ?<br>Назовите основные задачи обеспечения информационной безопасности РФ. Какие из них требуют безотлагательного решения? | ПК-19 |
| | Каким требованиям должна удовлетворять система безопасности предприятия?<br>Что является компонентами комплексной модели информационной безопасности?<br>Перечислите виды объектов защиты.<br>Назовите возможные пути утраты информации.<br>Дайте характеристику основным элементы системы защиты предприятия.<br>Что такое защитные действия?<br>Приведите классификацию защитных действий. | ПК-20 |
| | Как осуществляется отнесение информации к государственной тайне? В соответствии с какими нормативно-правовыми документами?<br>В соответствии с какими принципами происходит отнесение информации к государственной тайне?<br>Что является основанием для рассекречивания секретных сведений?<br>Назовите формы допуска к секретным сведениям. Доступ к какой по степени секретности информации имеет право гражданин, у которого первая форма допуска?<br>Какие особенности имеет режим секретности?<br>Какие по содержанию мероприятия включает в себя режим секретности?<br>Для чего создаются ПДТК на предприятии? | ПК-21 |
| | Какие документы положены в основу работы ПЗГТ? | ПК-22 |

| | | |
|---|---|---|
| | Приведите классификацию информации по режиму доступа. | |
| | Виды криптосистем. Задачи, решаемые методами криптографии.<br>Виды информации, подлежащие закрытию, их модели и свойства. Частотные характеристики открытых сообщений.<br>Критерии на открытый текст. Особенности нетекстовых сообщений. | ПК-23 |
| | Подпись RSA, Эль-Гамаля.<br>Подпись Фиата-Шамира.<br>Подпись Онга-Шнорра-Шамира.<br>Неотрицаемая подпись Шаума-ван-Антверпена.<br>Стандарты ЭЦП: DSS, ГОСТ Р 34.10-94.<br>Эллиптическая кривая над конечным полем. Операции на эллиптической кривой. Сумма точек. Кратная точка. | ПК-24 |
| | Композиции шифров. Enigma. Шифр Хейглина.<br>Математическая модель шифра.<br>Атаки и угрозы шифрам.<br>Блочные шифры и их ключевая система. Замены и перестановки.<br>Сеть Файстеля. Шифры DES, ГОСТ 28147-89.<br>Шифр AES<br>Шифр IDEA. | ПК-25 |
| | Какие функции должна выполнять служба безопасности по проверке сотрудников предприятия на благонадежность?<br>Какие методы сбора информации о гражданине могут использовать сотрудники службы безопасности предприятия?<br>В чем состоит особенность проверки благонадежности кандидатов на замещение руководящих должностей? | ПК-26 |
| | Какие виды действий могут выполнять сотрудники службы безопасности в соответствии с законом РФ “О частной детективной и охранной деятельности”?<br>Назовите известные в природе средства переноса информации?<br>Какова структура переноса информации? | ПК-27 |
| | Понятие и классификация средств защиты информации. Назначение программных, криптографических и технических средств защиты.<br>Дайте определение понятию информационная безопасность.<br>Перечислите основные составляющие информационной безопасности. | ПК-28 |
| | Что такое сертификат на средство защиты информации? Для чего он нужен?<br>Назовите нормативно-правовые документы РФ, являющиеся базой лицензирования и сертификации в области защиты информации.<br>Какие государственные органы РФ уполномочены на ведение лицензионной деятельности в области защиты информации? | ПСК-7.1 |
| | Что следует сделать для того, чтобы исключить неправомерное овладение конфиденциальной информацией?<br>Что является основными целями защиты информации в информационных системах?<br>Что представляет собой разглашение защищаемой информации?<br>В каких случаях возможно разглашение конфиденциальной информации? | ПСК-7.2 |
| | Перечислите основные методы обеспечения информационной безопасности РФ и кратко охарактеризуйте их.<br>Какова структура государственной системы обеспечения | ПСК-7.3 |

| | | |
|---|---|---|
| | информационной безопасности РФ?<br>Что включают организационные методы защиты информации?<br>На что направлена деятельность по защите информации?<br>Какие задачи обеспечения информационной безопасности решаются на организационном уровне?<br>Что такое система безопасности предприятия?<br>На основе каких принципов осуществляется функционирование системы безопасности предприятия? | |
| | Назовите способы НСД к охраняемым сведениям конфиденциального характера.<br>Дайте определения понятиям, используемым для организации работ с информацией, относимой к государственным секретам, таким как государственная тайна, система защиты государственной тайны, гриф секретности, степень секретности.<br>Приведите примеры информации, относимой к государственным секретам.<br>Какая информация не может быть отнесена к государственной тайне? | ПСК-7.4 |
| | Что такое коммерческая тайна?<br>На основе каких критериев происходит отнесение информации к коммерческой тайне предприятия?<br>Как происходит оформление допуска сотрудников предприятия к коммерческой тайне?<br>Что такое служба безопасности предприятия? Приведите типовую организационную структуру службы безопасности. | ПСК-7.5 |

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

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

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

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

10.2. Фонд оценочных средств для оценки защиты ВКР

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

Описание показателей для оценки компетенций для ВКР и ее защиты:

– актуальность темы ВКР;

– научная обоснованность предложений и выводов;

– использование производственной информации и методов решения инженерно–технических, организационно–управленческих и экономических задач;

– теоретическая и практическая значимость результатов работы и/или исследования;

– полнота и всестороннее раскрытие темы ВКР;

– соответствие результатов работы и/или исследования поставленным цели и задачам в ВКР;

– соответствие оформления ВКР установленным требованиям;

– умение четко и ясно доложить содержание ВКР;

– умение обосновать и отстаивать принятые решения;

– умение отвечать на поставленные вопросы;

– знание передового отечественного и зарубежного опыта;

– уровень самостоятельности выполнения работы и обоснованность объема цитирования;

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

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

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

Таблица 12 –Критерии оценки уровня сформированности компетенций

| Оценка компетенции (4–балльная шкала) | Характеристика сформированных компетенций |
|---|---|
| «отлично» | – студент глубоко и всесторонне усвоил учебный материал ОП, уверенно, логично, последовательно и грамотно его излагает;<br>– опираясь на знания основной и дополнительной литературы, студент свободно привязывает усвоенные научные положения к практической деятельности, обосновывая выдвинутые предложения;<br>– студент умело обосновывает и аргументирует выбор темы ВКР и выдвигаемые им идеи;<br>– студент аргументировано делает выводы;<br>– прослеживается четкая корреляционная зависимость между поставленными целью и задачами и полученными результатами работы и/или исследования;<br>– студент свободно владеет системой специализированных понятий;<br>– содержание доклада, иллюстративно–графического материала (при наличии) студента полностью соответствует содержанию ВКР;<br>– студент соблюдает требования к оформлению ВКР и иллюстративно–графического материала (при наличии);<br>– студент четко выделяет основные результаты своей профессиональной деятельности и обосновывает их |

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

| | |
|---|---|
| | профессиональной деятельности и не обосновывает их теоретическую и практическую значимость;<br>– студент отступает от регламента выступления;<br>– студент сбивчиво и не уверено излагает материалы доклада;<br>– отсутствует логика в ответах студента на поставленные членами ГЭК вопросы;<br>– студент не точно использует профессиональную терминологию при защите ВКР. |
| «неудовлетворительно»* | – студент не усвоил учебный материал ОП, при его изложении допускает неточности;<br>– допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении;<br>– студент не может обосновать выбор темы ВКР;<br>– студент не может сформулировать выводы;<br>– слабая зависимость между поставленными целью и задачами и полученными результатами работы и/или исследования;<br>– студент не владеет системой специализированных понятий;<br>– содержание доклада и иллюстративно–графического материала (при наличии) студента не полностью соответствует содержанию ВКР;<br>– студент не соблюдает требования к оформлению ВКР и иллюстративно–графического (при наличии) материала;<br>– студент не выделяет основные результаты своей профессиональной деятельности и не может обосновать их теоретическую и практическую значимость;<br>– студент не соблюдает регламент выступления;<br>– отсутствует аргументированность при изложении материалов доклада;<br>– отсутствует ясность в ответах студента на поставленные членами ГЭК вопросы;<br>– студент не грамотно использует профессиональную терминологию при защите ВКР;<br>– содержание ВКР не соответствует установленному уровню оригинальности. |

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

10.2.2. Перечень тем ВКР

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

10.2.3. Уровень оригинальности содержания ВКР составляет не менее «65» %.

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

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

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

Приложение № 1

Перечень тем ВКР на 2021/22 учебный год, 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 направлению подготовки/специальности «10.05.05 «Безопасность информационных технологий в правоохранительной сфере» от работодателя

В соответствии с требованиями Федерального государственного образовательного стандарта высшего образования (ФГОС ВО) – 10.05.05 «Безопасность информационных технологий в правоохранительной сфере» (уровень подготовки кадров высшей квалификации), утвержден приказом Приказом Министерства образования и науки РФ от 19 декабря 2016 г. N 1612, «Государственная итоговая аттестация» осуществляется в рамках блока Б3 «Государственная итоговая аттестация» учебного плана.

Разработчиком рабочей программы дисциплины (РПД) «*Государственная итоговая аттестация*» является заведующий кафедры №54 «Технологий защиты информации», д.т.н. Беззатеев С.В.

В рассматриваемую РПД включены следующие элементы:

1. Цели осуществления «*Государственной итоговой аттестации*».
2. Цели осуществления «*Государственной итоговой аттестации*» соотнесены с общими целями основной образовательной программы (ООП), в том числе: имеют междисциплинарный характер, связанны с задачами воспитания.
3. Прописана связь «*Государственной итоговой аттестации»* с другими дисциплинами учебного плана по ООП.
4. Прописан вклад «*Государственной итоговой аттестации»* при формировании компетенций (ОК, ОПК, ПК): по ФГОС ВО по направлению; по ООП.
5. При формировании требований при осуществлении «*Государственной итоговой аттестации)*» учтены результаты обучения, приведенные во ФГОС ВО по направлению.
6. Содержание дисциплины структурировано по видам учебных занятий с указанием их объемов.
7. Расчет времени в программе соответствует объему часов, отведенному на изучение дисциплины по учебному плану.
8. Указано учебно-методическое обеспечение дисциплины, в том числе: - перечень основной и дополнительной литературы, электронных ресурсов - методические рекомендации (материалы) преподавателю; методические рекомендации студентам.
9. Указаны формы текущего, промежуточного и итогового контроля.
10. Приведены фонды оценочных средств (ФОС): вопросы для проверки качества знаний студентов.
11. К процессу разработки и актуализации РПД и учебно-методических материалов дисциплины привлекаются работодатели, ориентированные на выпускников программы: *предоставление исходных материалов для анализа и расчетных программ.*

**Недостатки не выявлены.**

РПД ***«Государственная итоговая аттестация»*** может быть использована для методического обеспечения учебного процесса в рамках основной образовательной программы по направлению подготовки основной образовательной программы по направлению 10.05.05 «Безопасность информационных технологий в правоохранительной сфере».

Рецензент:

# 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 |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |