МИНИСТЕРСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ ПО ДЕЛАМ ГРАЖДАНСКОЙ ОБОРОНЫ, ЧРЕЗВЫЧАЙНЫМ СИТУАЦИЯМ И ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ СТИХИЙНЫХ БЕДСТВИЙ

**Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Санкт-Петербургский университет
Государственной противопожарной службы МЧС России»**

ПРОГРАММА
ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

**Специалитет по специальности
10.05.03 – Информационная безопасность автоматизированных систем**

Специализация «Анализ безопасности информационных систем»

Санкт-Петербург

1. Общие положения

1.1 Целью государственной итоговой аттестации является определение соответствия результатов освоения обучающимися основных профессиональных образовательных программ соответствующим требованиям федерального государственного образовательного стандарта по направлению специальности 10.05.03 – Информационная безопасность автоматизированных систем направленность, специализация «Анализ безопасности информационных систем».

1.2 Государственная итоговая аттестация (ГИА) обучающихся проводится в форме:

- государственного экзамена;
- защиты выпускной квалификационной работы.

1.3 Трудоемкость ГИА составляет 9 зачетных единиц.

2. Перечень планируемых результатов освоения образовательной программы

Выпускник, допущенный к сдаче экзамена, должен продемонстрировать владение следующими компетенциями:

Таблица 2.1

Наименование категории (группы) универсальных компетенций	**Формируемая универсальная компетенция**	**Индикатор достижения компетенции**
Системное и критическое мышление	УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.1. Использует методы критического анализа и системного подхода; методики разработки стратегии действий для выявления и решения проблемных ситуаций; инструменты для решения задач/проблем профессиональной деятельности
		УК-1.2. Анализирует и систематизирует разнородные данные, оценивает эффективность процедур анализа проблем и принятия решений в профессиональной деятельности
		УК-1.3. Обладает навыками системного и критического мышления; методиками постановки цели, определения способов ее достижения; методами принятия решений
Разработка и реализация проектов	УК-2. Способен управлять проектом на всех этапах его жизненного цикла	УК-2.1. Определяет этапы жизненного цикла проекта; виды ресурсов и ограничений для решения проектных задач; необходимые для осуществления проектной деятельности правовые нормы и принципы управления проектами, цифровые инструменты, предназначенные для разработки проекта/решения задачи; методы и программные средства управления проектами
		УК-2.2. Формирует целевые этапы, основные направления работ; объясняет цели и формулирует задачи, связанные с подготовкой и реализацией проекта; выдвигает альтернативные варианты действий с целью выработки новых оптимальных алгоритмов действий по проекту
		УК-2.3. Использует навыки управления проектом на всех этапах его жизненного цикла; навыками решения профессиональных задач в условиях цифровизации общества
Командная работа и лидерство	УК-3. Способен организовывать и руководить работой команды, вырабатывая командную	УК-3.1. Определяет типологии и факторы формирования команд, способы социального взаимодействия; цели, задачи, функции и структуру управления; организацию и стиль работы руководителя; соотношение целей и средств в моральной деятельности сотрудников; нравственные отношения в служебном коллективе (начальник – подчиненный, взаимоотношения между сотрудниками); служебный

Наименование категории (группы) универсальных компетенций	Формируемая универсальная компетенция	Индикатор достижения компетенции
	стратегию для достижения поставленной цели	этикет: основные принципы и формы; управление рисками, управление конфликтами; систему мотивации труда, стимулирование служебно-трудовой активности и воспитание подчиненных
		УК-3.2. Действует в духе сотрудничества; принимает решения с соблюдением морально-этических принципов и норм взаимоотношения в коллективе; проявляет уважение к мнению и культуре других; определяет цели и работать в направлении личностного и профессионального роста
		УК-3.3. Использует навыки распределения ролей в условиях командного взаимодействия; методы оценки своих действий, планирования и управления временем
Коммуникация	УК-4. Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	УК-4.1. Понимает принципы построения устного и письменного высказывания на государственном и иностранном языках; требования к деловой устной и письменной коммуникации
		УК-4.2. Демонстрирует способности применять на практике устную и письменную деловую коммуникацию
		УК-4.3. Использует методику составления суждения в межличностном деловом общении на государственном и иностранном языках, с применением адекватных языковых форм и средств, учитывая культурные традиции и профессиональную сферу
Межкультурное взаимодействие	УК-5. Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	УК-5.1. Понимает основные категории философии, законы исторического развития, основы межкультурной коммуникации
		УК-5.2. Ведет коммуникацию в мире культурного многообразия и демонстрирует взаимопонимание между представителями различных культур с соблюдением этических и межкультурных норм
		УК-5.3. Обладает навыками определения особенностей менталитета, обусловленных спецификой историко-культурного контекста; навыками интерпретации ценностных ориентиров общества в процессе межкультурного взаимодействия
Самоорганизация и саморазвитие (в том числе здоровьесбережение)	УК-6. Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни	УК-6.1. Понимает основные принципы самовоспитания и самообразования, исходя из квалификационных требований, требований рынка труда и перспектив развития профессиональной сферы
		УК-6.2. Обладает навыками самоконтроля и рефлексии, позволяющими самостоятельно корректировать саморазвитие по выбранной траектории
		УК-6.3. Владеет способами управления своей познавательной деятельностью и удовлетворения профессиональных интересов и потребностей
	УК-7. Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности	УК-7.1.Использует основные виды физических упражнений; научно-практические основы физической культуры и здорового образа и стиля жизни; нормативы физической и пожарно-прикладной (строевой) подготовки
		УК-7.2. Применяет на практике разнообразные средства физической культуры, спорта и туризма для сохранения и укрепления здоровья, психофизической подготовки и самоподготовки к будущей жизни и профессиональной деятельности; использовать творчески средства и методы физического воспитания для профессионально-личностного развития, физического самосовершенствования, формирования здорового образа и стиля жизни
		УК-7.3. Владеет средствами и методами укрепления индивидуального

Наименование категории (группы) универсальных компетенций	Формируемая универсальная компетенция	Индикатор достижения компетенции
		здоровья, физического самосовершенствования
Безопасность жизнедеятельности	УК-8. Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов	УК-8.1. Понимает причины, признаки и последствия опасностей, способов защиты от чрезвычайных ситуаций; основы безопасности жизнедеятельности; меры оказания первой помощи пострадавшим; основы организации и функционирования технической службы; нормативно- правовые акты в области гражданской обороны и особенности их подготовки
		УК-8.2. Выявляет причины и условия возникновения чрезвычайных ситуаций; оценивает вероятность возникновения потенциальной опасности для населения и территорий и принимает меры по ее предупреждению; обеспечивает техническую готовность пожарной, аварийно-спасательной техники и оборудования; проводит аварийно-спасательные работы
		УК-8.3. Использует методы прогнозирования возникновения опасных или чрезвычайных ситуаций; навыки поддержания безопасных условий жизнедеятельности; навыки оказания первой помощи пострадавшим в зависимости от патологии; навыки по организации и осуществлению надзорной деятельности в области пожарной безопасности
		УК-8.4. Выявляет и предупреждает угрозы безопасности личности общества и государства, применяет знания организационно-правовых основ использования огнестрельного оружия
Экономическая культура, в том числе финансовая грамотность	УК-9. Способен принимать обоснованные экономические решения в различных областях жизнедеятельности	УК-9.1. Обладает знаниями базовых принципов функционирования экономики и экономического развития, целей и форм участия государства в экономике, понятийного аппарата теории принятия решений и этапов выработки решений на операцию; классов задач принятия и поиска решений
		УК-9.2. Применяет методы личного экономического и финансового планирования для достижения текущих и долгосрочных финансовых целей, используя методы поиска решений, контролируя собственные экономические и финансовые риски
		УК-9.3. Принимает обоснованные экономические решения путем оценки их эффективности в профессиональной деятельности
Гражданская позиция	УК-10. Способен формировать нетерпимое отношение к коррупционному поведению	УК-10.1. Понимает основы национальной стратегии противодействия коррупции, основные законодательные и нормативно-правовые акты, регламентирующие ответственность за коррупционные правонарушения; особенности и основные категории профессиональной этики: долг, честь, совесть и справедливость, моральный выбор и моральную ответственность сотрудника (работника)
		УК-11.2. Идентифицирует действия коррупционной направленности при выполнении служебных обязанностей
		УК-11.3. Обладает навыками антикоррупционной агитации как информационного средства противодействия коррупции

Формируемая компетенция	Индикатор достижения компетенции
ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных	ОПК-1.1. Использует современные достижения отечественной и зарубежной науки и техники в области информационных технологий и информационной безопасности
	ОПК-1.2. Определяет значение информационных технологий и информационной безопасности для целей государства и общества
	ОПК-1.3. Оценивает и анализирует необходимость внедрения средств автоматизации и информационной безопасности в процессы профессиональной деятельности

Формируемая компетенция	Индикатор достижения компетенции
потребностей личности, общества и государства	
ОПК-2. Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности	ОПК-2.1. Понимает состав, классификацию, особенности функционирования современных информационных технологий и программных средств, в том числе отечественного производства при решении задач профессиональной деятельности
	ОПК-2.2. Выбирает современные информационные технологии и программные средства, в том числе отечественного производства для решения задач профессиональной деятельности
	ОПК-2.3. Применяет современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности
ОПК-3. Способен использовать математические методы, необходимые для решения задач профессиональной деятельности	ОПК-3.1. Применяет основные понятия и законы естественных наук, методы математического анализа и моделирования; основные методы теоретического и экспериментального исследования объектов, процессов и явлений
	ОПК-3.2. Использует физико-математический аппарат для разработки математических моделей явлений, процессов и объектов при решении инженерных задач в профессиональной деятельности; применять методы математического анализа и моделирования для обоснования принятия решений в профессиональной деятельности
	ОПК-3.3. Демонстрирует способности проведения экспериментов по заданной методике и анализа их результатов
ОПК-4. Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности	ОПК-4.1. Понимает физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники
	ОПК-4.2. Применяет основные физические законы и модели для решения задач профессиональной деятельности
	ОПК-4.3. Демонстрирует навыки анализа физических явлений и процессов функционирования микроэлектронной техники для решения задач профессиональной деятельности
ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	ОПК-5.1. Использует основные нормативные правовые акты, стандарты и методические документы в области защиты информации и информационной безопасности
	ОПК-5.2. Применяет нормативные акты при проектировании и разработке систем безопасности автоматизированных информационных систем и их компонентов
	ОПК-5.3. Демонстрирует навыки работы с нормативными документами, государственными и международными стандартами в области информационной безопасности и защиты информации
ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ОПК-6.1. Понимает меры защиты информации ограниченного доступа в автоматизированных системах; содержание нормативных правовых актов, нормативных и методических документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю
	ОПК-6.2. Определяет меры для организации защиты информации ограниченного доступа в автоматизированных системах и разрабатывает организационно-распорядительные документы, регламентирующие защиту информации ограниченного доступа в автоматизированных системах, в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю
	ОПК-6.3. Применяет действующую нормативную базу, нормативные и методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю для организации защиты информации ограниченного доступа в автоматизированных системах

Формируемая компетенция	Индикатор достижения компетенции
ОПК-7. Способен создавать программы на языках общего назначения, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ	ОПК-7.1. Использует алгоритмические основы программирования на языках общего назначения; языки программирования общего назначения; методы, реализуемые в современных инструментальных средствах программирования
	ОПК-7.2. Осуществляет обоснованный выбор способов организации программ и инструментария программирования при решении профессиональных задач; решает стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением средств и методов программирования и с учетом основных требований информационной безопасности
	ОПК-7.3. Демонстрирует навыки разработки алгоритмов для последующего создания программ на языках общего назначения; навыками использования типовых инструментальных средств программирования для решения профессиональных задач
ОПК-8. Способен применять методы научных исследований при проведении разработок в области защиты информации в автоматизированных системах	ОПК-8.1. Использует методы и процессы научных исследований, структуру научного знания, требования к научным разработкам; основные перспективы развития науки и техники в области профессиональной деятельности для проведения разработок в области защиты информации в автоматизированных системах
	ОПК-8.2. Формулирует задачи исследования, выбирает методы и средства их решения; проводит научные исследования в области информационной безопасности и защиты информации в автоматизированных информационных системах
	ОПК-8.3. Обладает навыками научно-исследовательской работы при проектировании и моделировании систем защиты информации
ОПК-9. Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации	ОПК-9.1. Демонстрирует знания основных информационных технологий, их состояния и тенденций развития; технических каналов утечки информации, основ технической защиты информации, основных характеристик и принципов построения средств технической защиты информации; принципов построения и функционирования сетей и систем передачи данных в профессиональной деятельности
	ОПК-9.2. Проводит анализ архитектуры и структуры сетей и систем передачи информации, оценивает эффективность архитектурно-технических решений, реализованных при построении сетей и систем передачи информации; применяет средства защиты от утечки по техническим каналам при решении задач профессиональной деятельности
	ОПК-9.3. Обладает навыками реализации вычислительных процедур и инструментального контроля показателей технической защиты информации, навыками эксплуатации систем и сетей передачи информации при решении задач профессиональной деятельности
ОПК-10. Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-10.1. Понимает основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации; основные методы и средства технической защиты информации; особенности применения криптографических и технических методов и средств защиты информации для решения задач профессиональной деятельности
	ОПК-10.2. Анализирует программные модели средств криптографической защиты информации, осуществляет подбор средств технической защиты информации для решения задач профессиональной деятельности
	ОПК-10.3. Применяет различные криптографические средства защиты информации и средства технической защиты для решения задач профессиональной деятельности
ОПК-11. Способен разрабатывать компоненты систем защиты информации автоматизированных систем	ОПК-11.1. Использует особенности проектирования автоматизированных информационных систем, методы и средства проектирования подсистем защиты информации, структуры и компонентов информационных систем
	ОПК-11.2. Проектирует и разрабатывает математическое и программное обеспечение автоматизированных информационных систем с учетом реализации требований информационной безопасности
	ОПК-11.3. Оценивает и обосновывает критерии эффективности функционирования защищенных автоматизированных информационных систем; разрабатывает

Формируемая компетенция	Индикатор достижения компетенции
	требования информационной безопасности к компонентам систем защиты информации автоматизированных систем
ОПК-12. Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем	ОПК-12.1. Использует теоретические основы построения баз данных, модели данных, принципы организации вычислительных сетей, сетевые технологии, технические средства их реализации, организации и виды операционных систем
	ОПК-12.2. Реализовывает политику безопасности компьютерной сети; анализирует, подбирает и применяет эффективные средства обеспечения безопасности баз данных при разработке автоматизированных систем
	ОПК-12.3. Демонстрирует навыки эксплуатации и администрирования систем управления базами данных и компьютерных сетей с учетом требований по обеспечению информационной безопасности при разработке автоматизированных систем
ОПК-13. Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем	ОПК-13.1. Использует модели угроз и рисков информационной безопасности автоматизированных систем, методы оценки уязвимостей каналов передачи информации
	ОПК-13.2. Проводит тестирование информационной безопасности автоматизированных систем на основе оценки рисков реализации угроз безопасности
	ОПК-13.3. Обладает навыками комплексного всестороннего анализа информационной безопасности автоматизированных информационных систем и их отдельных элементов
ОПК-14. Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений	ОПК-14.1. Понимает содержание исходных данных, необходимых для разработки автоматизированных систем, основные этапы жизненного цикла автоматизированных систем, меры по защите информации в автоматизированных системах; угрозы и атаки, характерные для автоматизированных систем
	ОПК-14.2. Разрабатывает, внедряет и осуществляет эксплуатацию автоматизированных систем и подсистем их безопасности с учетом требований по защите информации, выявляет уязвимости информационно-технологических ресурсов автоматизированных систем, проводит подготовку исходных данных для технико-экономического обоснования проектных решений
	ОПК-14.3. Демонстрирует навыки подбора программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы
ОПК-15. Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем	ОПК-15.1. Использует методы и инструментальные средства администрирования и контроля систем защиты автоматизированных систем
	ОПК-15.2. Осуществляет мониторинг и периодический контроль функционирования средств и систем защиты информации
	ОПК-15.3. Применяет инструментальные средства мониторинга и анализа состояния системы информационной безопасности
ОПК-16. Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма	ОПК-16.1. Понимает основные закономерности исторического процесса, этапы исторического развития России, место и роль России в истории человечества и в современном мире
	ОПК-16.2. Формулирует и аргументировано отстаивает собственную позицию по различным проблемам истории России
	ОПК-16.3. Использует принципы историзма и научной объективности как основу формирования собственной гражданской позиции и развития патриотизма

Формируемая компетенция	Индикатор достижения компетенции
ОПК-7.1 Способен использовать программные и программно-аппаратные средства для моделирования и испытания систем защиты информационных систем	ОПК-7.1.1. Использует программные и программно-аппаратные средства в качестве компонентов систем защиты информации автоматизированных систем, типовые архитектуры и принципы построения современных защищенных информационных систем
	ОПК-7.1.2. Осуществляет рациональный подбор состава программных и программно-аппаратных средств для моделирования и испытания систем защиты информационных систем
	ОПК-7.1.3. Обладает навыками администрирования и тестирования подсистем защиты информации автоматизированных систем
ОПК-7.2 Способен разрабатывать методики и тесты для анализа степени защищенности информационной системы и ее соответствия нормативным требованиям по защите информации	ОПК-7.2.1. Использует знания источников и классификации угроз информационной безопасности; нормативные документы, стандарты, содержащие рекомендации и требования по использованию методов и средств защиты информации; методы и средства анализа программного обеспечения информационных систем
	ОПК-7.2.2. Демонстрирует способности применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности для анализа степени защищенности информационной системы; проводить мониторинг угроз безопасности компьютерных сетей и систем
	ОПК-7.2.3. Обладает навыками формирования требований по защите информации информационных систем; настройки систем передачи данных и тестирования информационных систем
ОПК-7.3 Способен проводить анализ защищенности и верификацию программного обеспечения информационных систем	ОПК-7.3.1. Использует методы и средства анализа программного обеспечения; основы построения защищенных информационных систем
	ОПК-7.3.2. Анализирует и оценивает угрозы информационной безопасности в информационных системах
	ОПК-7.3.3. Применяет методы и средства анализа безопасности и верификации программного обеспечения; навыки разработки безопасного программного обеспечения информационных систем
ПК-1. Способен проводить анализ уязвимостей и эффективности средств и способов защиты информации в автоматизированных системах на основе методов моделирования	ПК-1.1 Использует методологические основы, методы и средства моделирования в области информационной безопасности; методы построения и исследования математических моделей в области информационной безопасности; методы планирования и оптимизации компьютерных экспериментов в области информационной безопасности, методы решения оптимизационных задач различных классов с учетом особенностей компьютерной реализации алгоритмов и анализа алгоритмической сложности; ПК-1.2 Демонстрирует навыки построения и исследования формализованных моделей в области информационной безопасности; применения языков моделирования, программных и аппаратных средства исследования эффективности технологических процессов обработки информации; решения основных типов оптимизационных задач в области информационной безопасности; ПК-1.3 Разрабатывает и исследует формализованные модели в сфере информационной безопасности; разрабатывает и исследует технологические процессы обработки и анализа информации в автоматизированных системах; формирует оптимальные решения в области информационной безопасности
ПК-2. Способен проводить инструментальный мониторинг защищенности информации в компьютерных системах и сетях	ПК-2.1 Использует основные понятия мониторинга событий, методы сбора информации о событиях, принципы работы систем управления информацией и событиями безопасности; ПК-2.2 Демонстрирует навыки сбора и анализа информации о событиях информационной безопасности для целей мониторинга информационной безопасности; ПК-2.3 Применяет методы мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем
ПК-3. Способен оценивать работоспособность и эффективность применяемых программно-аппаратных средств защиты информации	ПК-3.1 Использует методики обеспечения надежности и безопасности программно-аппаратных средств защиты информации; принципы функционирования информационно-коммуникационных систем; критерии оценки эффективности и надежности средств защиты информации автоматизированных систем; знания последствий от нарушения свойств безопасности информации; знания криптографических алгоритмов и особенностей их программной реализации; ПК-3.2 Выполняет аудит основных функциональных возможностей программно-

Формируемая компетенция	Индикатор достижения компетенции
	аппаратных средств защиты информации; проводит проверку работоспособности и эффективности применяемых программно-аппаратных средств защиты информации; ПК-3.3 Демонстрирует навыки выбора наилучшей конфигурации информационной системы; анализа данных о функционировании программно-аппаратных средств защиты информации
ПК-4. Способен формировать требования к защите информации в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры	ПК-4.1. Руководствуется требованиями нормативных правовых актов в области защиты информации значимых объектов критической информационной инфраструктуры; основами построения и функционирования современных и перспективных автоматизированных систем управления МЧС России; методикой формирования моделей нарушителей и методику оценки угроз безопасности информации значимых объектов критической информационной инфраструктуры; методы и средства обеспечения безопасности значимых объектов критической информационной инфраструктуры; ПК-4.2. Проводит анализ исходных данных и проектных решений при разработке подсистем и средств обеспечения безопасности значимых объектов критической информационной инфраструктуры; использует комплексы технических средств автоматизации управления подразделении МЧС России; определяет источники угроз безопасности информации и проводит оценку возможностей нарушителей по реализации угроз безопасности информации; планирует и разрабатывает организационно-правовые и программно-технические меры по обеспечению безопасности значимых объектов критической информационной инфраструктуры; ПК-4.3. Демонстрирует навыки проектирования подсистем безопасности значимых объектов критической информационной инфраструктуры; использования комплексов технических средств автоматизации деятельности подразделений МЧС России
ПК-5. Способен моделировать и исследовать технологии по автоматизации информационно-аналитической деятельности в сфере безопасности	ПК-5.1. Использует методологические основы и принципы организации информационно-аналитической деятельности; основные принципы и проблематику теории машинного обучения; методы машинного обучения; ПК-5.2. Применяет современные методы и средства автоматизированного сбора, обработки и анализа информации в области технологии автоматизации информационно-аналитической деятельности; реализовывает основные алгоритмы теории машинного обучения оценивает их точность и эффективность; ПК-5.3. Анализирует современные тенденции развития технологий автоматизации информационно-аналитической деятельности; использует отечественный и зарубежный опыт применения стандартов в области защиты информации в информационно-аналитических системах; применения основных технологий, методов, используемых при разработке интеллектуальных программных компонентов автоматизированных информационно-аналитических систем
ПК-6. Способен разрабатывать проектные решения по защите информации в автоматизированных системах	ПК-6.1. Применяет правила лицензирования и сертификации в области защиты информации; международные законодательные акты и договоры о защите персональных данных; Федеральное законодательство России в области защиты персональных данных; ПК-6.2. Демонстрирует способности построения частной модели угроз для информационной системы обработки персональных данных; классификации информационной системы обработки персональных данных; ПК-6.3. Разрабатывает частное техническое задание на систему защиты информационной системы обработки персональных данных

В результате освоения основной профессиональной образовательной программы обучающийся должен продемонстрировать владение УК, ОПК, ПК, представленные в таблице 2.1 и способность использовать профессиональные компетенции при решении профессиональных задач соответствующих видов деятельности, представленных в таблице 2.2.

Таблица 2.2

Типы задач профессиональной деятельности	Профессиональные задачи	Планируемые результаты (коды формируемых компетенций)
проектный	Реализация информационных технологий в сфере профессиональной деятельности с использованием защищенных автоматизированных систем; Администрирование подсистем информационной безопасности автоматизированных систем; Мониторинг информационной безопасности автоматизированных систем; Управление информационной безопасностью автоматизированных систем	ПК-1 ПК-2 ПК-3
организационно-управленческий	Организация работы коллектива, принятие управленческих решений в условиях спектра мнений, определение порядка выполнения работ; Организационно-методическое обеспечение информационной безопасности автоматизированных систем; Организация работ по созданию, внедрению, эксплуатации и сопровождению защищенных автоматизированных систем; Контроль реализации политики информационной безопасности	ПК-4 ПК-5
эксплуатационный	Сбор и анализ исходных данных для проектирования защищенных автоматизированных систем; Разработка политик информационной безопасности автоматизированных систем; Разработка защищенных автоматизированных систем в сфере профессиональной деятельности; Обоснование выбора способов и средств защиты информационно-технологических ресурсов автоматизированных систем; Выполнение проектов по созданию программ, комплексов программ, программно-аппаратных средств, баз данных, компьютерных сетей для защищенных автоматизированных систем;	ПК-6

	Разработка систем управления информационной безопасностью автоматизированных систем	

3. Содержание государственного экзамена

Подготовка к сдаче и сдача государственного экзамена проводится в объеме 3 з.е.

Готовность к профессиональной деятельности проверяется через решение обучающимися задач профессиональной деятельности указанными выше в таблице 2.2.

В программу государственного экзамена по специальности 10.05.03 – Информационная безопасность автоматизированных систем направленность, специализация «Анализ безопасности информационных систем» включены примерные вопросы по дисциплинам: «Методы и средства криптографической защиты информации», «Программно-аппаратные средства защиты информации», «Сети и системы передачи информации», «Разработка и эксплуатация автоматизированных систем в защищенном исполнении», «Безопасность операционных систем».

4. Рекомендации по подготовке к государственному экзамену

При подготовке к государственному экзамену, которая имеет самостоятельный характер, выпускник должен ориентироваться на рабочие программы изученных дисциплин.

При подготовке к государственному экзамену, обучающиеся получают представление об основном содержании программы государственного экзамена.

Получив представление о содержании разделов программы, выпускник должен приступить к детальному изучению вопросов каждого раздела этой программы. При подготовке следует соблюдать последовательность в изучении изложенного материала в рабочих программах дисциплин, представленных на государственный экзамен.

Перед государственным экзаменом проводится консультация по программе государственного экзамена в объеме 2-х часов.

5. Оценочные материалы для проведения государственного экзамена

5.1. Перечень вопросов, выносимых на государственный экзамен

Вопросы к государственному междисциплинарному экзамену по дисциплине «**Методы и средства криптографической защиты информации**»

1. Шифр IDEA.
2. Подходы к криптоанализу блочных шифров.
3. Дифференциальный криптоанализ.
4. Линейный криптоанализ.
5. Режимы шифрования.

6. Многократное шифрование.
7. Композиция блочных шифров.
8. Совершенные шифры.
9. Пример совершенного шифра.
10. Энтропийные характеристики шифров.
11. Идеальные шифры.
12. Избыточность языка.
13. Оценка числа ложных ключей и расстояние единственности.
14. Безусловно стойкие и вычислительно стойкие шифры.
15. Псевдослучайные последовательности (ПСП).
16. Характеристики генераторов ПСП (ПСГ).
17. Требования к криптографическим ПСП.
18. Примеры ПСГ и криптографических ПСГ.
19. Поточные шифры.
20. Общая схема поточного шифра.
21. Синхронные и самосинхронизирующиеся шифры.
22. Регистры сдвига с обратной линейной связью (РСЛОС).
23. ПСГ на основе РСЛОС.
24. Шифр A5.
25. Нелинейные регистры сдвига.
26. Шифр RC4.
27. Теория имитостойкости Симмонса.
28. Имитация и подмена сообщения.
29. Характеристики имитостойкости.
30. Совершенная имитостойкость.
31. Коды аутентификации сообщений.
32. Защитные контрольные суммы.
33. Криптографические хэш-функции и требования к ним.
34. Подходы к проектированию хэш-функций.
35. Хэш-функции на основе блочного шифра.
36. Ключевые хэш-функции.
37. Понятие односторонней функции и односторонней функции с "лазейкой".
38. Проблемы факторизации целых чисел и логарифмирования в конечных полях.
39. Криптосистема Диффи-Хэллмана. Пример.
40. Криптосистема RSA. Пример.
41. Криптосистема Эль-Гамаля. Пример.
42. Криптосистема Рабина. Пример.
43. Криптосистема Гольдвассер-Микали. Пример.
44. Криптосистема Блюма-Гольдвассер. Пример.
45. Рюкзачные шифры.
46. Криптосистема Меркла-Хэллмана.
47. Понятие электронной цифровой подписи и требования к ней.
48. Атаки и угрозы схемам ЭЦП.
49. Подпись RSA, Эль-Гамаля.

50.Подпись Фиата-Шамира.
51. Подпись Онга-Шнорра-Шамира.
52.Неотрицаемая подпись Шаума-ван-Антверпена.
53.Стандарты ЭЦП: DSS, ГОСТ Р 34.10-94.
54.Эллиптическая кривая над конечным полем.
55.Операции на эллиптической кривой.
56.Сумма точек. Кратная точка.
57.Проблема дискретного логарифмирования на эллиптической кривой.
58. Переход от шифра (ЭЦП) в Zp к шифру (ЭЦП) на эллиптической кривой.
59. Шифр Эль-Гамаля на эллиптической кривой.
60.Стандарты ЭЦП на эллиптической кривой: ГОСТ Р 34.10- 2001, ECDSA.

Вопросы к государственному междисциплинарному экзамену по дисциплине «**Программно-аппаратные средства защиты информации**»

1. Основные понятия и определения в области защиты компьютерной информации.
2. Современная ситуация в области защиты компьютерной информации.
3. Требования к системам защиты информации.
4. Понятие угрозы безопасности компьютерной информации. Интервал потенциальной опасности.
5. Классификация угроз безопасности компьютерной информации.
6. Источники, риски и формы атак на информацию.
7. Принципы защиты компьютерной информации
8. Идентификация субъекта, понятие протокола идентификации, идентифицирующая информация
9. Основные подходы к защите данных от НСД (контроль доступа и разграничение доступа, иерархический доступ к файлу)
10. Формальные модели управления доступом
11. Классификация средств защиты компьютерной информации от НСД
12. Аутентификация пользователей. Основные алгоритмы (протоколы) аутентификации.
13. Администрирование сетей в аспекте безопасности информации
14. Защита сетевого файлового ресурса, фиксация доступа к файлам.
15. Доступ к данным со стороны процесса, способы фиксации факта доступа.
16. Надежность систем ограничения доступа
17. Защита файлов от изменения
18. Электронная цифровая подпись (ЭЦП)
19. Методы и средства ограничения доступа к компонентам ЭВМ
20. Программно-аппаратные средства шифрования
21. Построение аппаратных компонент криптозащиты данных
22. Защита алгоритма шифрования
23. Принцип чувствительной области и принцип главного ключа
24. Пароли и ключи, организация хранения ключей

25. Необходимые и достаточные функции аппаратного средства криптозащиты
26. Защита программ от несанкционированного копирования
27. Защита программ от изучения
28. Защита программ от отладки, защита от дизассемблирования
29. Защита программ от трассировки по прерываниям
30. Защита от разрушающих программных воздействий (РПВ)
31. Компьютерные вирусы как особый класс РПВ
32. Необходимые и достаточные условия недопущения разрушающего воздействия
33. Понятие изолированной программной среды
34. Общая характеристика и классификация вредоносных программ
35. Компьютерные вирусы. Классификация компьютерных вирусов
36. Основы технологии анализа защищенности компьютерных систем управления и обработки информации
37. Многоуровневая защита корпоративных сетей.

Вопросы к государственному междисциплинарному экзамену по дисциплине «**Сети и системы передачи информации**»

1. Алгоритм декодирования для обнаружения ошибок.
2. Особенности реализации алгоритма декодирования в современных системах.
3. Использование циклических кодов для обнаружения пакетов ошибок.
4. Оценка вероятности ошибки декодирования.
5. Использование имитационного моделирования для оценки вероятности ошибок декодирования.
6. Выбор числа экспериментов
7. Вычисление верхней оценки для вероятности ошибки декодирования. Вычисление вероятности ошибки декодирования.
8. Передача данных по каналу с обратной связью.
9. Базовая модель системы передачи с обратной связью.
10. Учет ошибок в обратном канале.
11. Учет задержки в получении квитанции.
12. Алгоритм с ожиданием.
13. Использование циклов регенерации для оценки коэффициента использования канала
14. Алгоритм с возвратом.
15. Алгоритм с селективным повторением.
16. Альтернативные подходы для организации повторных передач в канале с задержкой.
17. Алгоритм с виртуальными каналами.
18. Алгоритм передачи по каналу с высокой вероятностью ошибки.
19. Семиуровневая модель взаимодействия открытых вычислительных систем.
20. Понятие протокола и интерфейса.

21. Классификация методов управления доступом к среде.
22. Основные сведения из теории массового обслуживания.
23. Простейшие системы массового обслуживания.
24. Синхронная система с постоянным временем обслуживания.
25. Анализ доступа с разделением времени на качественном уровне.
26. Анализ доступа по запросу на качественном уровне.
27. Сравнение доступа по запросу и доступа с разделением времени.
28. Базовая модель системы со случайным множественным доступом в канале.
29. Алгоритм случайного множественного доступа.
30. Алгоритм Алоха.
31. Разновидности алгоритма Алоха (оптимальный алгоритм Алоха, адаптивная Алоха, алгоритм двоичной экспоненциальной отсрочки).
32. Особенности реализации алгоритма Алоха и его разновидностей (вероятностный и интервальный варианты).
33. Особенности работы алгоритма Алоха и его разновидностей в системе с большим числом абонентов.
34. Древовидные алгоритмы разрешения конфликтов.
35. Среднее время разрешения конфликта в стек-алгоритме.
36. Работа алгоритмов случайного множественного доступа в канале с шумами.
37. Работа алгоритма Алоха в канале с ложными конфликтами.
38. Работа стек-алгоритма в канале с ложными конфликтами.
39. Особенности реализации алгоритмов случайного множественного доступа в современных локальных сетях передачи данных.
40. Упрощенный анализ алгоритмов множественного доступа для локальных сетей.
41. Физический уровень.
42. Разбиение физического уровня на подуровни.
43. Подуровень модуляционного кодирования.
44. Примеры модуляционных кодов.
45. Подуровень сопряжения со средой и физическая среда.
46. Сетевой уровень.
47. Классификация IP-адресов.
48. Структура IP-пакета.
49. Маршрутизация в сети internet.
50. Понятие маршрутных таблиц.
51. Организация unicast и multicast-передачи.
52. Понятие о MAC-адресах.
53. Соответствие между IP и MAC-адресами.
54. Транспортный уровень. UDP-протокол.
55. Упрощенное описание структуры UPD-пакетов.
56. Служебные протоколы сети internet.
57. Использования ICMP-протокола для анализа характеристик сети.
58. TCP-протокол. Основная идея TCP-протокола.
59. Перегрузка сети при работе TCP-протокола.

60. Алгоритм медленного старта.
61. Оценка коэффициента использования канала для TCP-протокола.
62. Уровни, расположенные выше транспортного.
Выделение на прикладном уровне специального подуровня. RTP-протокол.

Вопросы к государственному междисциплинарному экзамену по дисциплине «**Разработка и эксплуатация автоматизированных систем в защищенном исполнении**»

1. Понятие, виды и структура автоматизированных систем (по РД 50-680-88)
2. Безопасность АС, ее составляющие.
3. Основные способы и механизмы обеспечения безопасности информации в АС
4. Классификация, идентификация (инвентаризация, каталогизация) и оценивание (категорирование) объектов защиты в АС
5. Классификация (каталогизация), идентификация, спецификация и оценивание угроз безопасности в АС
6. Человеческий фактор в угрозах безопасности.
7. Модель нарушителя безопасности информации в АС (РД Гостехкомиссии
8. Декомпозиция назначения, целей и задач ОПК- функционирования АС.
9. Функциональная структура АС и функциональные требования к защищенным СВТ, АС, продуктам и системам ИТ
10. Система и структура функциональных требований по защите от НСД к информации в СВТ (по РД Гостехкомиссии), классы защищенности СВТ
11. Система и структура функциональных требований по защите от НСД в АС (по РД Гостехкомиссии), группы и классы защищенности АС
12. Общая структура требований безопасности к изделиям и системам ИТ, классы функциональных требований безопасности (по ГОСТ Р ИСО/МЭК 15408-2002. Ч.2)
13. Услуги (сервисы) безопасности при взаимодействии открытых систем и механизмы безопасности, их реализующие (по ГОСТ Р ИСО 7498-1-99), взаимоотношение между услугами защиты и уровнями взаимодействия по 7-ми уровневой эталонной модели ВОС
14. Жизненный цикл, стадии создания и содержание работ по созданию АС, особенности создания АС в защищенном исполнении (по ГОСТ 34.601-90, ГОСТ Р 51583)
15. Техническое задание на создание АС, требования по структуре, содержанию, порядку разработки, оформления, согласования и утверждения (по ГОСТ 34.602-89)
16. Особенности Технического задания на создание АС в защищенном исполнении.
17. Составляющие общих требований к АСЗИ и структуру функциональных требований (по ГОСТ Р 51624)

18. Жизненный цикл изделий (продуктов и систем) ИТ, общая схема и последовательность создания изделий ИТ

19. Классификация изделий ИТ и функциональные пакеты требований безопасности. Классы защищенности изделий ИТ и пакеты требований доверия безопасности (по ГОСТ Р ИСО/МЭК 15408-2002 и РД Гостехкомиссии)

20. Структура, порядок разработки, регистрации и опубликования профилей защиты для изделий ИТ (по ГОСТ Р ИСО/МЭК 15408-2002 и РД Гостехкомиссии)

21. Структура, назначение и порядок разработки задания по безопасности при создании изделий ИТ, соотношение между профилем защиты и заданием по безопасности.

22. Техническое задание на создание системы ИТ (по ГОСТ Р ИСО/МЭК 15408-2002 и РД Гостехкомиссии)

23. Содержание процесса разработки и ввода в действие изделий (систем) ИТ.

24. Уровни представления проектных решений

25. Проектирование АС как особый вид деятельности, объекты проектирования при создании АС (по РД 50-680- 88)

26. Методология (методы и средства) проектирования АС

27. Каноническое (индивидуальное) проектирование АС.

28. Технологическая схема этапов технического и рабочего проектирования

29. Типовое проектирование АС и его методы.

30. Технологическая схема проектирования

31. Управление процессом проектирования АС, его компоненты и специфика

32. Организационная структура, схемы организации работ при проектировании АС и организационные формы проектного коллектива

33. Содержание и специфика управленческого цикла при проектировании АС

34. Методы планирования и управления проектами.

35. Диаграммы Гантта, сетевые графики проектов

36. Автоматизированные системы управления проектами

37. Общие положения по эксплуатации изделий, комплексов, средств деятельности.

38. Составляющие организационных и технических мероприятий по эксплуатации

39. Особенности эксплуатации КС (АС) и защищенных КС (АС в защищенном исполнении).

40. Администрирование КС (АС)

41. Органы управления и планирования эксплуатации защищенных АС

42. Эксплуатационная документация на АС (изделия ИТ).

43. Руководства пользователя и администратора

44. Конструкторские эксплуатационные документы на ТСО и ПО, эксплуатационные документы предприятия

Вопросы к государственному междисциплинарному экзамену по дисциплине «**Безопасность операционных систем**»

1. Понятие виртуальной памяти
2. Страничное распределение виртуальной памяти
3. Сегментное распределение виртуальной памяти
4. Странично-сегментное распределение виртуальной памяти
5. Свопинг
6. Назначение и функции файловой системы
7. Логическая организация файловой системы
8. Файловая система FAT
9. Файловая система NTFS
10. Контроль доступа к файлам
11. Основные понятия безопасности ОС
12. Системный подход к обеспечению безопасности
13. Симметричные криптосистемы
14. Асимметричные криптосистемы
15. Аутентификация
16. Аутентификация на основе многоразовых паролей
17. Аутентификация на основе одноразовых паролей
18. Цифровые сертификаты
19. Цифровые подписи
20. Авторизация доступа
21. Аудит
22. Средства администрирования ОС Windows Server
23. Средства безопасности ОС Windows Server
24. Планирование и диспетчеризация потоков
25. Алгоритмы планирования
26. Управление памятью
27. Управление доступом в Linux
28. Управление доступом в Windows
29. Анализ операционных систем
30. Средства аутентификации операционных систем
31. Управление средствами аутентификации в Linux
32. Управление средствами аутентификации в Windows
33. Документирование политики безопасности
34. Централизованное планирование политики безопасности в лесу доменов Windows
35. Централизованное планирование политики безопасности в Linux

5.2. Критерии оценки результатов сдачи государственного экзамена

Таблица 5.1

Шкала оценивания	Критерии оценивания
отлично	- обучающийся демонстрирует знание классических и

	инновационных теоретических подходов к решению профессиональных задач; - излагает материал в логической последовательности, научным языком с использованием соответствующей терминологии, обоснованными выводами, ответ содержит обращение к собственному опыту или примеры из практического опыта; - уровень усвоения компетенций показывает сформированные системные знания, сформированные навыки и умения и их успешную актуализацию.
хорошо	- обучающийся демонстрирует знание основных теоретических подходов к решению профессиональных задач; излагает материал в логической последовательности, научным языком с использованием соответствующей терминологии, обоснованными выводами, ответ содержит обращение к собственному опыту или примеры из практического опыта. При ответе были допущены неточности; - уровень усвоения компетенций показывает сформированные, но содержащие отдельные пробелы знания, успешно применяемые навыки и умения.
удовлетворительно	- обучающийся демонстрирует частичное знание теоретических подходов к решению профессиональных задач; при изложении материала допущены две-три ошибки и/или нарушена последовательность, при ответе обучающийся затруднялся в пояснении терминов; - уровень усвоения компетенций показывает фрагментарные знания, частично освоенные навыки и умения.
неудовлетворительно	- обучающийся демонстрирует слабое знание теоретических подходов к решению профессиональных задач; при изложении материала допускает больше трех ошибок; не владеет научной терминологией, отсутствуют примеры практического опыта; - уровень усвоения компетенций показывает ограниченные знания, слабо сформированные навыки и умения.

6. Перечень рекомендуемой литературы для подготовки к государственному экзамену

Перечень рекомендуемой литературы для подготовки к государственному экзамену по дисциплине «Методы и средства криптографической защиты информации»

Основная литература:

1. Шаньгин, В. Ф. Информационная безопасность [Текст]: научно-популярная литература / В. Ф. Шаньгин. - М.: ДМК Пресс, 2014. - 702 с

2. Рябко, Б. Я. Криптографические методы защиты информации [Текст] : учебное пособие / Б. Я. Рябко, А. Н. Фионов. - 2-е изд., стер. - М. : Горячая линия - Телеком, 2014. - 229 с

Дополнительная литература:

1. Титов, А.А. Инженерно-техническая защита информации [Электронный ресурс]: учебное пособие. — Электрон. дан. — М.: ТУСУР (Томский

государственный университет систем управления и радиоэлектроники), 2010. — 195 с.
2. Шнайер Б. Прикладная криптография. – М.: Вильямс, 2016. – 1024 с.
3. Смарт Н. Криптография. – М.: Техносфера, 2006. – 528 с.

Перечень рекомендуемой литературы для подготовки к государственному экзамену по дисциплине «Программно-аппаратные средства защиты информации»

Основная литература:

1. Романова И. К. Управление сложными техническими объектами: учеб. пособие / Романова И. К.; МГТУ им. Н. Э. Баумана. - М.: Изд-во МГТУ им. Н. Э. Баумана, 2010. Ч. 3: Построение математических моделей систем. - 2010. - 68 с.: ил. - Библиогр.: с. 68.
2. Платонов В. В. Программно-аппаратные средства защиты информации : учебник для вузов / Платонов В. В. - М. : Академия, 2013. - 330 с.: ил. - (Высшее профессиональное образование. Бакалавриат). - Библиогр.: с. 326-327. - ISBN 978-5-7695- 9327-7.

Дополнительная литература:

1. Белкин П.Ю., Михальский О.О., Першаков А.С. и др. Защита программ и данных: Учебное пособие для ВУЗов. - М.: Радио и связь, 1999.
2. Джеймс С. Амстронг, Секреты UNIX //Москва, Диалектика, 2000.
3. Лукацкий А.В. Обнаружение атак - СПб.: БХВ-Петербург, 2001.

Перечень рекомендуемой литературы для подготовки к государственному экзамену по дисциплине «Сети и системы передачи информации»

Основная литература:

1. Богомолова Н. Е. Системы и сети связи: учеб. пособие для вузов / Богомолова Н. Е. ; МГТУ им. Н. Э. Баумана. - М. : Изд-во МГТУ им. Н. Э. Баумана, 2007. - 121 с. : ил. - Библиогр. в конце кн. - ISBN 978-5-7038-3011-6.
2. Галкин В. А., Григорьев Ю. А. Телекоммуникации и сети : учеб. пособие для вузов / Галкин В. А., Григорьев Ю. А. - М. : Изд-во МГТУ им. Н. Э. Баумана, 2003. - 607 с. - (Информатика в техническом университете). - Библиогр.: с. 595-596. - ISBN 5-7038-1961- X.

Дополнительная литература:

1. Таненбаум Э. Д. Уэзеролл. Компьютерные сети, 6-е изд. СПБ.: Питер, 2016. 960 с.
2. Гольдштейн Б.С, Кучерявый А.Е. Сети связи пост- NGN. СПБ.: Питер, 2013. 159 с.
3. Б.С. Гольдтейн, Н.А. Соколов, Г.Г Яновский. Сети связи. «БХВ-Петербург», 2011, 399 с.

Перечень рекомендуемой литературы для подготовки к государственному экзамену по дисциплине «Разработка и эксплуатация автоматизированных систем в защищенном исполнении»

Основная литература:

1. Безопасность информационных систем и защита информации в МЧС России: учебное пособие: [гриф МЧС] / Ю.И. Синещук [и др.]; ред. В.С. Артамонов; С.-Петерб. гос. ун-т гос. противопож. службы МЧС России. – СПб.: СПбУ ГПС МЧС России, 2012. – 300 с. Режим доступа: http://elib.igps.ru/?4&type=card&cid=ALSFR-6d86bbe6-aeac-49db-bc2e-068c7a55cb8d&remote=false

2. Синещук, Ю.И. Информационные технологии и защита информации в автоматизированных системах управления МЧС России: учебное пособие для слушателей: [гриф МЧС] / Ю.И. Синещук, С.Н. Терехин, В.В. Духанин; ред. В.С. Артамонов; МЧС России. – СПб.: СПбУ ГПС МЧС России, 2010. – 284 с. – Режим доступа: http://elib.igps.ru/?6&type=card&cid=ALSFR-a2e62800-d42d-4e9c-9bc9-4c1d7b9f0f55&remote=false

Дополнительная литература:

1. Проектирование информационных систем [Электронный ресурс]: учебное пособие / С. Ю. Золотов. – Электрон. текстовые данные. – Томск: Томский государственный университет систем управления и радиоэлектроники, Эль Контент, 2013. – 88 с. – 978-5-4332-0083-8. – Режим доступа: http://www.iprbookshop.ru/13965.html

2. Меры защиты информации на уровне пользователя информационно-технологическими средствами: методические указания к самостоятельной работе студентов. Учебно-методическое пособие / Б. А. Бурняшов. – Саратов: Вузовское образование, 2014. – 55 с. – ISBN 2227-8397. http://www.iprbookshop.ru/23077.html

3. Буйневич, М.В. Основы кибербезопасности: способы анализа программ: учебное пособие для студентов высших учебных заведений, обучающихся по УГСН 10.00.00 "Информационная безопасность" по программам подготовки бакалавров, магистров, специалистов для слушателей: [гриф УМО] / М.В. Буйневич, К.Е. Израилов; МЧС России. – СПб.: СПбУ ГПС МЧС России, 2022. – 91 с. – ISBN 978-5-907489-42-4. Режим доступа: http://elib.igps.ru/?8&type=card&cid=ALSFR-00f64c85-4b2e-4cd4-bf09-6434a9411854&query=%D0%91%D1%83%D0%B9%D0%BD%D0%B5%D0%B2%D0%B8%D1%87&remote=false

Перечень рекомендуемой литературы для подготовки к государственному экзамену по дисциплине «Безопасность операционных систем»

Основная литература:

1. Батаев, А. В. Операционные системы и среды: учебник [для СПО] / А. В. Батаев, Н. Ю. Налютин, С. В. Синицын. - 4-е изд., стер. - Москва: Академия, 2020. - 272 с.: рис., табл. - (Профессиональное образование). - Библиогр.: с. 267 (19 назв.). - ISBN 978-5-4468-8681-4

2. Таненбаум, Э. Современные операционные системы [Текст] = Modern operating systems / Э. Таненбаум. - 3-е изд. - СПб.: ПИТЕР, 2015. - 1120 с

Дополнительная литература:

1. Филиппов А.А. Операционные системы: учебное пособие / Филиппов А.А.. — Ульяновск: Ульяновский государственный технический университет, 2021. — 100 с. — ISBN 978-5-9795-2129-9. — Текст: электронный // IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/121273.html

2. Олифер В., Олифер Н. Компьютерные сети. Принципы технологии протоколы. Юбилейное издание. Учебник – издательство «Питер», 2021. – 1008 с.

3. Платунова, С. М. Администрирование вычислительных сетей на базе MS Windows Server® 2008 R2 : учебное пособие — СПб. : Университет ИТМО, 2013. — 127 с. — Режим доступа: http://www.iprbookshop.ru/68640.html

7. Требования к выпускным квалификационным работам и порядку их выполнения

Подготовка к процедуре защиты и процедура защиты ВКР проводится в объеме (в зачетных единицах): 6 з.е.

7.1. Порядок выполнения и оформления выпускных квалификационных работ

Требования, предъявляемые к выполнению и оформлению выпускных квалификационных работ бакалавриата по направлению специальности 10.05.03 – Информационная безопасность автоматизированных систем направленность, специализация «Анализ безопасности информационных систем», определены Стандартом организации «Положение о выпускной квалификационной работе по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры».

7.2. Оценочные материалы для проведения защиты выпускных квалификационных работ

7.2.1. Примерная тематика выпускных квалификационных работ

1. Разработать пакет (состав и содержание) документов для создания объекта информатизации – автоматизированной системы в защищённом исполнении в ГУ субъекта РФ МЧС России.
2. Разработать пакет (состав и содержание) документов для создания объекта информатизации - защищаемого помещения в ГУ субъекта РФ МЧС России.

3. Разработать пакет (состав и содержание) документов для создания системы обработки и обеспечения безопасности персональных данных в ГУ субъекта РФ МЧС России.

4. Разработать пакет (состав и содержание) документов для аттестации объекта информатизации - защищаемого помещения по требованиям безопасности информации в ГУ субъекта РФ МЧС России.

5. Разработать пакет (состав и содержание) документов для создания объекта информатизации – автоматизированной системы по требованиям безопасности информации в ГУ субъекта РФ МЧС России.

6. Разработать пакет (состав и содержание) документов для создания объекта информатизации – информационной системы персональных данных в ГУ субъекта РФ МЧС России.

7. Разработать пакет (состав и содержание) документов для аттестации объекта информатизации – информационной системы персональных данных по требованиям безопасности информации в ГУ субъекта РФ МЧС России.

8. Разработать пакет (состав и содержание) документов для создания объекта информатизации – локальной вычислительной сети в защищённом исполнении в ГУ субъекта РФ МЧС России.

9. Разработать пакет (состав и содержание) документов для аттестации объекта информатизации – локальной вычислительной сети по требованиям безопасности информации в ГУ субъекта РФ МЧС России.

10. Совершенствование системы криптозащиты в узле связи МЧС России.

11. Оптимизация системы обслуживания защищаемых контуров локальной сети МЧС России.

12. Совершенствование автоматизированной системы в защищенном исполнении МЧС России.

7.2.2. Критерии защиты выпускных квалификационных работ

Шкала критериев оценивания:

Таблица 7.1

Шкала	Критерии
отлично	- содержание полностью раскрывает утвержденную тему и отличается высокой степенью актуальности и новизны, задачи, сформулированные обучающимся, решены в полном объеме; - выполненная работа свидетельствует о знании обучающимся большинства теоретических концепций по рассматриваемой проблематике; - в работе в полной мере использованы современные нормативные и литературные источники, а также обобщенные данные эмпирического исследования выпускника, теоретическое освещение вопросов темы сочетается с исследованием практики деятельности органов государственной власти и других организаций; - теоретические выводы и практические предложения по исследуемой проблеме вытекают из содержания работы,

	аргументированы, полученные результаты исследования значимы и достоверны, высока степень самостоятельности выпускника, работа носит творческий характер; - работу отличает четкая структура, завершенность, логичность изложения, оформление, соответствующее предъявляемым требованиям; - доклад о выполненной работе сделан методически грамотно; - результаты исследования представляют интерес для практического использования в деятельности органов государственной власти и других организаций; - уровень усвоения компетенций показывает сформированные системные знания, сформированные навыки и умения и их успешную актуализацию
хорошо	- содержание работы актуально, в целом раскрывает утвержденную тему; - выполненная работа свидетельствует о знании обучающимся основных теоретических концепций по рассматриваемой проблематике; - в работе использован основной круг современных нормативных и литературных источников, а также обобщенные данные практической деятельности; - теоретические выводы и практические предложения по исследуемой проблеме в целом вытекают из содержания работы, аргументированы, работа носит самостоятельный характер, однако имеются отдельные недостатки в изложении некоторых вопросов, неточности, спорные положения; - основные вопросы изложены логично, оформление работы соответствует предъявляемым требованиям; - при защите обучающийся относительно привязан к тексту доклада, но в целом способен представить полученные результаты; - уровень усвоения компетенций показывает сформированные, но содержащие отдельные пробелы знания, успешно применяемые навыки и умения
удовлетворительно	- содержание работы в значительной степени раскрывает утвержденную тему, вместе с тем отдельные вопросы изложены без должного теоретического обоснования, исследование проведено поверхностно; - выполненная работа свидетельствует о недостаточном знании обучающимся основных теоретических концепций по рассматриваемой проблематике; - современные нормативные и литературные источники использованы не в полном объеме, данные практической деятельности органов государственной власти и других организаций использованы фрагментарно; - выводы и предложения по исследуемой проблеме поверхностны, недостаточно обоснованы и не подкреплены обобщенными данными эмпирического исследования, имеются неточности, спорные положения; - оформление работы в целом соответствует предъявляемым требованиям; при защите автор работы привязан к тексту доклада, испытывает затруднения при ответах на отдельные вопросы;

	- уровень усвоения компетенций показывает фрагментарные знания, частично освоенные навыки и умения
неудовлетворительно	- содержание работы не раскрывает утвержденную тему, обучающийся не проявил навыков самостоятельной работы, оформление работы не соответствует предъявленным требованиям, выявлены недобросовестные заимствования, в процессе защиты работы обучающийся показывает слабые знания по исследуемой теме, не отвечает на поставленные вопросы; - уровень усвоения компетенций показывает ограниченные знания, слабо сформированные навыки и умения

Автор: д.т.н., профессор Буйневич М.В.