Федеральное агентство морского и речного транспорта
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«Государственный университет морского и речного флота
имени адмирала С.О. Макарова»**
Воронежский филиал ФГБОУ ВО «ГУМРФ имени адмирала С.О. Макарова»

Кафедра математики, информационных систем и технологий

«УТВЕРЖДАЮ»
И.о. директора филиала
_____ Е.Ф. Глинкина
«__» _____ 20__ г.

**Дополнительная профессиональная образовательная программа
профессиональной переподготовки**

«Информационная безопасность»

Объем программы – 520 часов
Форма обучения - очная, заочная

Воронеж 2025

Содержание

1. Общие положения

Нормативная основа дополнительной профессиональной образовательной программы:

Федеральный закон от 29.12.2012 № 273-ФЗ (ред. от 02.07.2021) «Об образовании в Российской Федерации»

Приказ Минобрнауки России от 01.07.2013 № 499 (ред. от 15.11.2013) «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам»

Приказ Минобрнауки России от 23.08.2017 № 816 «Об утверждении Порядка применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ»

Приказ Минтруда России от 14.09.2022 № 525н «Об утверждении профессионального стандарта «Специалист по защите информации в автоматизированнх системах»

Цель: совершенствование профессиональных компетенций и (или) освоение новых компетенций, необходимых для профессиональной деятельности, и (или) повышение профессионального уровня в области обеспечения информационной безопасности.

Задачи:

применять на практике требования нормативных правовых актов, методических документов, международных и национальных стандартов в области ТЗКИ ;

разрабатывать необходимые документы в интересах проведения работ по ТЗКИ ;

определять возможные ТКУИ и угрозы безопасности информации в результате НСД и специальных воздействий ;

формировать требования по ТЗКИ, определять требования к средствам ТЗКИ на объектах информатизации ;

организовывать и проводить работы по ТЗКИ, по контролю (мониторингу) защищенности конфиденциальной информации, оформлять материалы по результатам контроля ;

применять на практике штатные средства ТЗКИ и средства контроля (мониторинга) эффективности мер защиты информации ;

проводить аттестационные испытания и аттестацию объектов информатизации на соответствие требованиям по защите информации, оформлять материалы аттестационных испытаний ;

разрабатывать программы и методики аттестационных испытаний и аттестации объектов информатизации ;

осуществлять аутентификацию взаимодействующих объектов, проверку подлинности отправителя и целостности передаваемых данных ;

проводить установку, монтаж, испытания и техническое обслуживание средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации ;

определять категории значимости объектов КИИ ;

обосновывать организационные и технические меры, подлежащие реализации в рамках системы безопасности значимого объекта КИИ ;

формировать сведения о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких ка-

тегорий ;

выявлять и анализировать угрозы безопасности информации по результатам оценки возможностей внешних и внутренних нарушителей ;

разрабатывать документы для получения лицензии на проведение работ и оказания услуг по ТЗКИ для их представления в лицензирующий орган ;

определять виды и типы средств защиты информации, обеспечивающих реализацию технических мер в рамках системы безопасности значимого объекта КИИ ;

определять структуру системы безопасности значимого объекта КИИ ;

осуществлять выбор средств защиты информации с учетом их стоимости, совместимости с применяемыми программными и программно-аппаратными средствами, функций безопасности средств и особенностей их реализации, а также категории значимого объекта КИИ ;

определять требования к параметрам настройки программных и программно-аппаратных средств, наличия средств защиты информации, обеспечивающих реализацию мер по обеспечению безопасности, а также устранение возможных уязвимостей, приводящих к возникновению угроз безопасности информации ;

определять требования к обеспечению безопасности значимого объекта КИИ.

К освоению программы допускаются лица:

– имеющие высшее профессиональное или среднее профессиональное образования;

– получающие высшее профессиональное или среднее профессиональное образование.

Категория слушателей: руководители и специалисты структурных подразделений по защите информации и информационной безопасности, подразделений информационных технологий, подразделений, ответственных за организацию конфиденциального, в том числе электронного, документооборота органов государственной власти, органов местного самоуправления и организаций (предприятий) различных организационных форм и форм собственности.

Срок обучения: 520 часов

Форма обучения – очная, заочная с применением дистанционных образовательных технологий

Характеристика профессиональной деятельности слушателей

Область профессиональной деятельности слушателей:

- Обеспечение безопасности информации в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости

Объектом профессиональной деятельности слушателей являются:

- Повышение защищенности автоматизированных систем, функционирующих в условиях существования угроз в информационной сфере и обладающих информационно-технологическими ресурсами, подлежащими защите, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости

2. Планируемые результаты освоения дополнительной профессиональной образовательной программы

Трудовая функция в соответствии с профессиональным стандартом	Перечень профессиональных компетенций	Необходимые умения	Необходимые знания	Разделы программы, формирующие профессиональные компетенции	Форма проверки сформированности компетенции
Проведение технического обслуживания систем защиты информации автоматизированных систем	Проверка работоспособности системы защиты информации автоматизированной системы Контроль соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации Контроль стабильности характеристик системы защиты информации автоматизированной системы	Конфигурировать параметры системы защиты информации автоматизированной системы в соответствии с ее эксплуатационной документацией Обнаруживать и устранять неисправности системы защиты информации автоматизированной системы согласно эксплуатационной документации Производить монтаж и диагностику компьютерных сетей Использовать типовые криптографические средства защиты информации, в том числе средства электронной подписи	Типовые средства и методы защиты информации в локальных и глобальных вычислительных сетях Базовая конфигурация системы защиты информации автоматизированной системы Особенности применения программных и программно-аппаратных средств защиты информации в автоматизированных системах Типовые средства, методы и протоколы идентификации, аутентификации и авторизации Нормативные правовые акты в области защиты информации Организационные меры по защите информации		
Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем	Ведение документов учета, обработки, хранения и передачи информации ограниченного доступа Информирование персонала об угрозах безопасности информации Информирование персонала о правилах эксплуатации системы защиты автоматизированной системы и отдельных средств защиты информации Ведение протоколов и журналов учета при изменении конфигурации систем защиты информации	Оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации Оформлять техническую документацию в соответствии с нормативными правовыми актами в области защиты информации	Нормативные правовые акты в области защиты информации Основные методические и руководящие документы федеральных органов исполнительной власти, уполномоченных в области обеспечения информационной безопасности, безопасности информации в ключевых системах информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации Эксплуатационная и проектная документация на автоматизированную систему Основные методы организации и		

Трудовая функция в соответствии с профессиональным стандартом	Перечень профессиональных компетенций	Необходимые умения	Необходимые знания	Разделы программы, формирующие профессиональные компетенции	Форма проверки сформированности компетенции
	автоматизированных систем Ведение протоколов и журналов учета при осуществлении мониторинга систем защиты информации автоматизированных систем Ведение протоколов и журналов учета при осуществлении аудита систем защиты информации автоматизированных систем Подготовка сведений об отсутствии необходимости присвоения категорий значимости объекту критической информационной инфраструктуры, на котором используется автоматизированная система, и направление в письменном виде этих сведений в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, по утвержденной им форме		проведения технического обслуживания технических средств информатизации Организационные меры по защите информации		
Обеспечение защиты информации при выводе из эксплуатации автоматизированных систем	Включение в организационно-распорядительные документы по защите информации процедур уничтожения (стирания) информации на машинных носителях, а также контро-	Использовать программные средства для архивирования информации Использовать программные и программно-аппаратные средства для уничтожения (стирания) информации и носителей информации	Процедуры архивирования информации, обрабатываемой автоматизированной системой Назначение и принципы работы основных узлов современных технических средств информатизации Организация технического обслу-		

Трудовая функция в соответствии с профессиональным стандартом	Перечень профессиональных компетенций	Необходимые умения	Необходимые знания	Разделы программы, формирующие профессиональные компетенции	Форма проверки сформированности компетенции
	ля уничтожения (стирания) информации Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) Физическое уничтожение машинных носителей информации, обрабатываемой автоматизированной системой Архивирование информации, обрабатываемой автоматизированной системой	Использовать типовые криптографические средства защиты информации, в том числе электронную подпись	живания и ремонта компонентов автоматизированной системы Процедуры уничтожения (стирания) информации на машинных носителях, а также контроля уничтожения (стирания) информации Нормативные правовые акты в области защиты информации Основные методические и руководящие документы уполномоченных федеральных органов исполнительной власти по защите информации		
Диагностика систем защиты информации автоматизированных систем	Обнаружение инцидентов в процессе эксплуатации автоматизированной системы Идентификация инцидентов в процессе эксплуатации автоматизированной системы Оценка защищенности автоматизированных систем с помощью типовых программных средств Устранение последствий инцидентов, возникших в процессе эксплуатации автоматизированной системы Расчет показателей эффективности защиты инфор-	Определять источники и причины возникновения инцидентов Оценивать последствия выявленных инцидентов Обнаруживать нарушения правил разграничения доступа Устранять нарушения правил разграничения доступа Осуществлять контроль обеспечения уровня защищенности в автоматизированных системах Использовать криптографические методы и средства защиты информации в автоматизированных системах	Нормативные правовые акты в области защиты информации Национальные, межгосударственные и международные стандарты в области защиты информации Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации Организационные меры по защите информации Принципы построения средств защиты информации от несанкционированного доступа и утечки по техническим каналам Критерии оценки защищенности автоматизированной системы Технические средства контроля эффективности мер защиты ин-		

Трудовая функция в соответствии с профессиональным стандартом	Перечень профессиональных компетенций	Необходимые умения	Необходимые знания	Разделы программы, формирующие профессиональные компетенции	Форма проверки сформированности компетенции
	мации, обрабатываемой в автоматизированных системах Инструментальный контроль показателей эффективности защиты информации, обрабатываемой в автоматизированных системах		формации Регламент информирования персонала автоматизированной системы о выявленных инцидентах Регламент учета выявленных инцидентов Регламент устранения последствий инцидентов Основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения защиты информации в автоматизированных системах		
Администрирование систем защиты информации автоматизированных систем	Установка обновлений программного обеспечения автоматизированной системы Выполнение установленных процедур обеспечения безопасности информации с учетом требования эффективного функционирования автоматизированной системы Управление полномочиями доступа пользователей автоматизированной системы Информирование пользователей о правилах эксплуатации автоматизированной системы с учетом требований по защите информации Проведение занятий с персоналом по работе с системой защиты информации автоматизированной системы, включая проведение	Создавать, удалять и изменять учетные записи пользователей автоматизированной системы Формировать политику безопасности программных компонентов автоматизированных систем Устанавливать и настраивать операционные системы, системы управления базами данных, компьютерные сети и программные системы с учетом требований по обеспечению защиты информации Использовать криптографические методы и средства защиты информации в автоматизированных системах Регистрировать события, связанные с защитой информации в автоматизированных системах Анализировать события, связанные с защитой информации в автоматизированных системах	Принципы формирования политики информационной безопасности в автоматизированных системах Программно-аппаратные средства защиты информации автоматизированных систем Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах Методы контроля эффективности защиты информации от утечки по техническим каналам Критерии оценки эффективности и надежности средств защиты программного обеспечения автоматизированных систем Технические средства контроля эффективности мер защиты информации Принципы организации и структура систем защиты программного обеспечения автоматизированных систем		

Трудовая функция в соответствии с профессиональным стандартом	Перечень профессиональных компетенций	Необходимые умения	Необходимые знания	Разделы программы, формирующие профессиональные компетенции	Форма проверки сформированности компетенции
	практических занятий с персоналом на макетах или в тестовой зоне Внесение изменений в эксплуатационную документацию и организационно-распорядительные документы по системе защиты информации автоматизированной системы		Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем безопасности автоматизированных систем Основные меры по защите информации в автоматизированных системах		
Управление защитой информации в автоматизированных системах	Анализ воздействия изменений конфигурации автоматизированной системы на ее защищенность Составление комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе Оценка последствий от реализации угроз безопасности информации в автоматизированной системе Анализ изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации	Оценивать информационные риски в автоматизированных системах Классифицировать и оценивать угрозы безопасности информации Определять подлежащие защите информационные ресурсы автоматизированных систем Применять нормативные документы по защите от несанкционированного доступа к информации и противодействию технической разведке Разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем Конфигурировать параметры системы защиты информации автоматизированных систем Применять технические средства контроля эффективности мер защиты информации	Основные методы управления защитой информации Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах Методы защиты информации от несанкционированного доступа и утечки по техническим каналам Нормативные правовые акты в области защиты информации Национальные, межгосударственные и международные стандарты в области защиты информации Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации		
Обеспечение работоспособности систем защиты информации при возникновении нештатных ситуаций	Обнаружение неисправностей в работе системы защиты информации автоматизированной системы	Применять типовые программные средства резервирования и восстановления информации в автоматизированных системах	Методы и способы обеспечения отказоустойчивости автоматизированных систем Содержание и порядок деятельно-		

Трудовая функция в соответствии с профессиональным стандартом	Перечень профессиональных компетенций	Необходимые умения	Необходимые знания	Разделы программы, формирующие профессиональные компетенции	Форма проверки сформированности компетенции
	Устранение неисправностей в работе системы защиты информации автоматизированной системы Резервирование программного обеспечения, технических средств, каналов передачи данных автоматизированной системы управления на случай возникновения нештатных ситуаций Создание альтернативных мест хранения и обработки информации на случай возникновения нештатных ситуаций Восстановление после сбоев и отказов программного обеспечения автоматизированных систем	Применять средства обеспечения отказоустойчивости автоматизированных систем Классифицировать и оценивать угрозы информационной безопасности Применять программные средства обеспечения безопасности данных Документировать действия по устранению неисправностей в работе системы защиты информации автоматизированной системы	сти персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем Основные информационные технологии, используемые в автоматизированных системах Принципы построения средств защиты информации от утечки по техническим каналам Программно-аппаратные средства обеспечения защиты информации автоматизированных систем Нормативные правовые акты в области защиты информации Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации Организационные меры по защите информации		
Мониторинг защищенности информации в автоматизированных системах	Выработка рекомендаций для принятия решения о модернизации системы защиты информации автоматизированной системы Выработка рекомендаций для принятия решения о повторной аттестации автоматизированной системы или о проведении дополнительных аттестационных испытаний Выявление угроз безопасности информации в автоматизированных системах Принятие мер защиты информации при выявлении	Классифицировать и оценивать угрозы информационной безопасности Анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах Применять нормативные документы по защите информации от несанкционированного доступа и противодействию технической разведке Контролировать эффективность	Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах Программно-аппаратные средства обеспечения защиты информации автоматизированных систем Методы защиты информации от		

Трудовая функция в соответствии с профессиональным стандартом	Перечень профессиональных компетенций	Необходимые умения	Необходимые знания	Разделы программы, формирующие профессиональные компетенции	Форма проверки сформированности компетенции
	новых угроз безопасности информации Анализ недостатков в функционировании системы защиты информации автоматизированной системы Устранение недостатков в функционировании системы защиты информации автоматизированной системы	принятых мер по реализации политик безопасности информации автоматизированных систем Контролировать события безопасности и действия пользователей автоматизированных систем Применять технические средства контроля эффективности мер защиты информации Документировать процедуры и результаты контроля функционирования системы защиты информации автоматизированной системы	утечки по техническим каналам Нормативные правовые акты в области защиты информации Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации Организационные меры по защите информации		
Аудит защищенности информации в автоматизированных системах	Оценка информационных рисков безопасности информации в автоматизированной системе Обоснование и контроль результатов управленческих решений в области безопасности информации автоматизированных систем Экспертиза состояния защищенности информации автоматизированных систем Обоснование критериев эффективности функционирования защищенных автоматизированных систем	Классифицировать и оценивать угрозы безопасности информации для объекта информатизации Разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем Разрабатывать политики безопасности информации автоматизированных систем Применять инструментальные средства контроля защищенности информации в автоматизированных системах	Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах Способы защиты информации от несанкционированного доступа и утечки по техническим каналам Методы контроля эффективности защиты информации от несанкционированного доступа и утечки по техническим каналам Принципы построения систем защиты информации Нормативные правовые акты в области защиты информации Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации Организационные меры по защите информации		
Установка и настройка	Входной контроль качества	Администрировать программные	Основные угрозы безопасности		

Трудовая функция в соответствии с профессиональным стандартом	Перечень профессиональных компетенций	Необходимые умения	Необходимые знания	Разделы программы, формирующие профессиональные компетенции	Форма проверки сформированности компетенции
средств защиты информации в автоматизированных системах	комплектующих изделий системы защиты информации автоматизированной системы Осуществление автономной наладки технических и программных средств системы защиты информации автоматизированной системы Проведение приемочных испытаний системы защиты информации автоматизированной системы Внесение в эксплуатационную документацию изменений, направленных на устранение недостатков, выявленных в процессе испытаний	средства системы защиты информации автоматизированных систем Устранять известные уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации Применять нормативные документы по защите информации от несанкционированного доступа и противодействию технической разведке Применять аналитические и компьютерные модели автоматизированных систем и систем защиты информации Проводить анализ структурных и функциональных схем защищенной автоматизированной системы Определять параметры настройки программного обеспечения системы защиты информации автоматизированной системы	информации и модели нарушителя в автоматизированных системах Содержание эксплуатационной документации автоматизированной системы Типовые средства, методы и протоколы идентификации, аутентификации и авторизации Основные меры по защите информации в автоматизированных системах Нормативные правовые акты в области защиты информации Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации		
Разработка организационно-распорядительных документов по защите информации в автоматизированных системах	Определение правил и процедур управления системой защиты информации автоматизированной системы Определение правил и процедур выявления инцидентов Определение правил и процедур мониторинга обеспечения уровня защищенности информации автоматизированной системы Определение правил и процедур защиты инфор-	Классифицировать и оценивать угрозы информационной безопасности Применять нормативные документы по защите информации от несанкционированного доступа и противодействию технической разведке Определять параметры настройки программного обеспечения системы защиты информации автоматизированной системы Контролировать эффективность принятых мер по защите информации в автоматизированных сис-	Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах Принципы построения средств защиты информации от несанк-		

Трудовая функция в соответствии с профессиональным стандартом	Перечень профессиональных компетенций	Необходимые умения	Необходимые знания	Разделы программы, формирующие профессиональные компетенции	Форма проверки сформированности компетенции
	мации при выводе автоматизированной системы из эксплуатации Определение правил и процедур реагирования на инциденты в автоматизированной системе	темах	ционированного доступа и утечки по техническим каналам Нормативные правовые акты в области защиты информации Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации		
Анализ уязвимостей внедряемой системы защиты информации	Выбор и обоснование критериев эффективности функционирования защищенных автоматизированных систем Проведение анализа уязвимости программных и программно-аппаратных средств системы защиты информации автоматизированной системы Проведение экспертизы состояния защищенности информации автоматизированных систем Уточнение модели угроз безопасности информации автоматизированной системы Проведение предварительных испытаний системы защиты информации автоматизированной системы Проведение анализа уязвимостей автоматизированных и информационных систем	Классифицировать и оценивать угрозы безопасности информации автоматизированной системы Разрабатывать предложения по совершенствованию системы управления защитой информации автоматизированной системы Проводить анализ доступных информационных источников с целью выявления известных уязвимостей, используемых в системе защиты информации программных и программно-аппаратных средств Устранять выявленные уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации	Основные методы и средства криптографической защиты информации Способы защиты информации от несанкционированного доступа и утечки по техническим каналам Способы контроля эффективности защиты информации от несанкционированного доступа и утечки по техническим каналам Нормативные правовые акты в области защиты информации Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации Организационные меры по защите информации Содержание эксплуатационной документации автоматизированной системы		
Внедрение организационных мер по защите инфор-	Проведение проверки полноты описания в организа-	Реализовывать правила разграничения доступа персонала к объек-	Нормативные правовые акты и национальные стандарты по ли-		

Трудовая функция в соответствии с профессиональным стандартом	Перечень профессиональных компетенций	Необходимые умения	Необходимые знания	Разделы программы, формирующие профессиональные компетенции	Форма проверки сформированности компетенции
мации в автоматизированных системах	ционно-распорядительных документах на автоматизированную систему действий персонала по реализации организационных мер защиты информации Проведение занятий с персоналом по работе с системой защиты информации автоматизированной системы, включая проведение практических занятий на макетах или в тестовой зоне Подготовка документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации Проведение проверки готовности персонала к эксплуатации системы защиты информации автоматизированной системы Подготовка документов, определяющих правила и процедуры контроля обеспеченности уровня защищенности информации, содержащейся в информационной системе Подготовка документов, определяющих правила и процедуры выявления инцидентов, которые могут привести к сбоям или нарушению функционирова-	там доступа Анализировать программные и программно-аппаратные решения при проектировании системы защиты информации с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах Консультирование персонала автоматизированной системы по комплексу мер (правилам, процедурам, практическим приемам, руководящим принципам, методам, средствам) обеспечения защиты информации Осуществлять планирование и организацию работы персонала автоматизированной системы с учетом требований по защите информации Конфигурировать аттестованную информационную систему и системы защиты информации информационной системы	цензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации Методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и систем защиты автоматизированных систем Нормативные правовые акты в области защиты информации Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации Организационные меры по защите информации Методики сертификационных испытаний технических средств защиты информации от несанкционированного доступа и утечки по техническим каналам на соответствие требованиям по безопасности информации Методы, способы и средства обеспечения отказоустойчивости автоматизированных информационных систем		

Трудовая функция в соответствии с профессиональным стандартом	Перечень профессиональных компетенций	Необходимые умения	Необходимые знания	Разделы программы, формирующие профессиональные компетенции	Форма проверки сформированности компетенции
	ния информационной системы и возникновению угроз безопасности информации Подготовка документов, определяющих правила и процедуры управления конфигурацией аттестованной информационной системы и системы защиты информации информационной системы				
Тестирование систем защиты информации автоматизированных систем	Проведение анализа структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем Выявление уязвимости информационно-технологических ресурсов автоматизированных систем Выявление основных угроз безопасности информации в автоматизированных системах Составление методик тестирования систем защиты информации автоматизированных систем Подбор инструментальных средств тестирования систем защиты информации автоматизированных сис-	Анализировать основные характеристики и возможности телекоммуникационных систем по передаче информации Анализировать основные узлы и устройства современных автоматизированных систем Применять действующую нормативную базу в области обеспечения безопасности информации Контролировать функционирование технических средств защиты информации Восстанавливать (заменять) отказавшие технические средства защиты информации	Принципы построения и функционирования систем и сетей передачи информации Эталонная модель взаимодействия открытых систем Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах Основные меры по защите информации в автоматизированных системах Особенности защиты информации в автоматизированных системах управления технологическими процессами Принципы построения средств защиты информации от несанкционированного доступа и утечки по техническим каналам Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах Технические каналы утечки информации		

Трудовая функция в соответствии с профессиональным стандартом	Перечень профессиональных компетенций	Необходимые умения	Необходимые знания	Разделы программы, формирующие профессиональные компетенции	Форма проверки сформированности компетенции
	тем Составление протоколов тестирования систем защиты информации автоматизированных систем		Технические средства контроля эффективности мер защиты информации Организационные основы защиты информации от несанкционированного доступа и утечки по техническим каналам на объектах информатизации Нормативные правовые акты в области защиты информации Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации Организационные меры по защите информации		
Разработка проектных решений по защите информации в автоматизированных системах	Разработка модели угроз безопасности информации и модели нарушителя в автоматизированных системах Разработка моделей автоматизированных систем и подсистем безопасности автоматизированных систем Разработка проектов нормативных документов, регламентирующих работу по защите информации Разработка предложений по совершенствованию системы управления безопасностью информации в автоматизированных системах	Применять действующую нормативную базу в области обеспечения защиты информации Применять нормативные документы по противодействию технической разведке Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности Определять типы субъектов доступа и объектов доступа, являющихся объектами защиты Определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в автоматизированной системе Выбирать меры защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы Определять виды и типы средств	Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации Нормативные правовые акты и национальные стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации Принципы построения и функционирования, примеры реализации современных локальных и глобальных компьютерных сетей и их компонентов Особенности защиты информации в автоматизированных системах управления технологическими процессами Критерии оценки эффективности и надежности средств защиты информации программного обеспе-		

Трудовая функция в соответствии с профессиональным стандартом	Перечень профессиональных компетенций	Необходимые умения	Необходимые знания	Разделы программы, формирующие профессиональные компетенции	Форма проверки сформированности компетенции
		защиты информации, обеспечивающих реализацию технических мер защиты информации Определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем	чения автоматизированных систем Принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем Основные характеристики технических средств защиты информации от несанкционированного доступа и утечек по техническим каналам Принципы формирования политики информационной безопасности в автоматизированных системах		
Разработка эксплуатационной документации на системы защиты информации автоматизированных систем	Анализ технической документации информационной инфраструктуры автоматизированной системы Анализ защищенности информационной инфраструктуры автоматизированной системы Формирование требований по защите информации, включая использование математического аппарата для решения прикладных задач Документирование программного обеспечения, технических средств, баз данных и компьютерных сетей с учетом требований по обеспечению защиты информации Анализ структурных и функциональных схем защищенных автоматизированных информационных	Определять меры (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации в автоматизированных системах Разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем Проектировать подсистемы безопасности информации с учетом действующих нормативных и методических документов Разрабатывать модели автоматизированных систем и систем защиты информации автоматизированных систем Исследовать модели автоматизированных систем и систем защиты безопасности автоматизированных систем Анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с	Основные методы управления информационной безопасностью Основные понятия теории автоматов, математической логики, теории алгоритмов и теории графов Основные методы управления проектами в области информационной безопасности Национальные, межгосударственные и международные стандарты в области защиты информации Основные меры по защите информации в автоматизированных системах Особенности защиты информации в автоматизированных системах управления технологическими процессами Угрозы безопасности, информационные воздействия, критерии оценки защищенности и методы защиты информации в автоматизированных системах Методы, способы, средства, последовательность и содержание		

Трудовая функция в соответствии с профессиональным стандартом	Перечень профессиональных компетенций	Необходимые умения	Необходимые знания	Разделы программы, формирующие профессиональные компетенции	Форма проверки сформированности компетенции
	систем Обоснование критериев эффективности функционирования защищенных автоматизированных информационных систем Применение программно-аппаратных средств обеспечения безопасности информации в автоматизированных системах	целью выявления потенциальных уязвимостей систем защиты информации автоматизированных систем Оценивать информационные риски в автоматизированных системах и определять информационную инфраструктуру и информационные ресурсы, подлежащие защите Проводить технико-экономическое обоснование проектных решений программно-аппаратных средств обеспечения защиты информации в автоматизированной системе с целью обеспечения требуемого уровня защищенности Исследовать эффективность проектных решений программно-аппаратных средств обеспечения защиты информации в автоматизированной системе с целью обеспечения требуемого уровня защищенности Проводить комплексное тестирование и отладку аппаратных и программных систем защиты информации	этапов разработки автоматизированных систем и систем защиты информации в автоматизированных системах Программно-аппаратные средства обеспечения защиты информации в программном обеспечении автоматизированных систем Основные средства, способы и принципы построения систем защиты информации автоматизированных систем Нормативные правовые акты в области защиты информации Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации		
Разработка программных и программно-аппаратных средств для систем защиты информации автоматизированных систем	Разработка технической документации на компоненты автоматизированных систем в соответствии с требованиями Единой системы конструкторской документации (далее - ЕСКД) и Единой системы программной документации	Разрабатывать технические задания на создание подсистем безопасности информации автоматизированных систем, проектировать такие подсистемы с учетом требований нормативных документов, ЕСКД и ЕСПД Анализировать программные, архитектурно-технические и схемо-	Профессиональная и криптографическая терминология в области безопасности информации Основные информационные технологии, используемые в автоматизированных системах Средства и способы обеспечения безопасности информации, принципы построения систем защиты		

Трудовая функция в соответствии с профессиональным стандартом	Перечень профессиональных компетенций	Необходимые умения	Необходимые знания	Разделы программы, формирующие профессиональные компетенции	Форма проверки сформированности компетенции
	(далее - ЕСПД) Синтез структурных и функциональных схем защищенных автоматизированных систем Разработка программного обеспечения, технических средств, баз данных и компьютерных сетей с учетом требований по обеспечению защиты информации Разработка электронных схем с учетом требований по защите информации Оптимизация работы электронных схем с учетом требований по защите информации	технические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах Проводить комплексное тестирование аппаратных и программных средств	информации Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах Современные технологии программирования Эталонная модель взаимодействия открытых систем, основные протоколы, последовательность и содержание этапов построения и функционирования современных локальных и глобальных компьютерных сетей Особенности защиты информации в автоматизированных системах управления технологическими процессами Принципы работы элементов и функциональных узлов электронной аппаратуры, типовые схемотехнические решения основных узлов и блоков электронной аппаратуры Принципы организации документирования разработки и процесса сопровождения программного и аппаратного обеспечения Методы тестирования и отладки программного и аппаратного обеспечения Архитектура, основные модели, последовательность и содержание этапов проектирования, физическая организация баз данных Нормативные правовые акты в области защиты информации Руководящие и методические до-		

Трудовая функция в соответствии с профессиональным стандартом	Перечень профессиональных компетенций	Необходимые умения	Необходимые знания	Разделы программы, формирующие профессиональные компетенции	Форма проверки сформированности компетенции
			кументы уполномоченных федеральных органов исполнительной власти по защите информации		
Обоснование необходимости защиты информации в автоматизированной системе	Анализ характера обрабатываемой информации и определение перечня информации, подлежащей защите Выявление степени участия персонала в обработке защищаемой информации Планирование мероприятий по обеспечению защиты информации в автоматизированной системе Определение требуемого класса (уровня) защищенности автоматизированной системы Обоснование необходимости использования криптографических средств защиты информации Разработка отчетных документов и разделов технических заданий	Анализировать цели создания автоматизированных систем и задачи, решаемые автоматизированными системами Выявлять уязвимости информационно-технологических ресурсов автоматизированных систем Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности и оценивать угрозы безопасности информации Организовывать работы по созданию, внедрению, проектированию, разработке и сопровождению защищенных автоматизированных систем Использовать рисковую методологию управления защитой информации в автоматизированной системе Определять класс защищенности автоматизированных систем и ее составных частей	Основные информационные технологии, используемые в автоматизированных системах Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах Виды информационных воздействий и критерии оценки защищенности информации в автоматизированных системах Методы защиты информации от несанкционированного доступа и утечки по техническим каналам Программно-аппаратные средства обеспечения защиты информации в программном обеспечении автоматизированных систем Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем Принципы формирования политики информационной безопасности в автоматизированных системах Нормативные правовые акты в области защиты информации Национальные, межгосударственные и международные стандарты в области защиты информации Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации Организационные меры по защите информации Методики сертификационных ис-		

Трудовая функция в соответствии с профессиональным стандартом	Перечень профессиональных компетенций	Необходимые умения	Необходимые знания	Разделы программы, формирующие профессиональные компетенции	Форма проверки сформированности компетенции
			пытаний технических средств защиты информации от несанкционированного доступа и утечки по техническим каналам на соответствие требованиям по безопасности информации Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации		
Определение угроз безопасности информации, обрабатываемой автоматизированной системой	Формирование разделов технических заданий на создание систем защиты информации автоматизированных систем Разработка систем защиты информации автоматизированных систем с учетом действующих нормативно-правовых документов Определение комплекса мер (правил, процедур, практических приемов, руководящих принципов, методов, средств) для защиты информации автоматизированных систем Определение оценки возможностей внешних и внутренних нарушителей Разработка модели угроз безопасности информации автоматизированной системы Обоснование перечня сертифицированных средств защиты информации, необ-	Производить выбор программно-аппаратных средств защиты информации для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности информации в автоматизированной системе Формировать перечень мероприятий по предотвращению угроз безопасности информации автоматизированной системы Систематизировать результаты проведенных исследований Анализировать возможные уязвимости информационных систем Выявлять известные уязвимости информационных систем Разрабатывать проекты нормативных документов, регламентирующих работу по защите информации в автоматизированных системах	Основные информационные технологии, используемые в автоматизированных системах Основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в вычислительных сетях Программно-аппаратные средства обеспечения защиты информации автоматизированных систем Способы реализации угроз безопасности в автоматизированных системах Последствия от нарушения свойств безопасности информации Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах Национальные, межгосударственные и международные стандарты в области защиты информации Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации Методики сертификационных ис-		

Трудовая функция в соответствии с профессиональным стандартом	Перечень профессиональных компетенций	Необходимые умения	Необходимые знания	Разделы программы, формирующие профессиональные компетенции	Форма проверки сформированности компетенции
	ходимых для создания системы защиты информации автоматизированной системы Анализ требований к назначению, структуре и конфигурации создаваемой автоматизированной системы с целью выявления угроз безопасности информации Определение структурно-функциональных характеристик информационной системы в соответствии с требованиями нормативных правовых документов в области защиты информации в автоматизированных системах		пытаний технических средств защиты информации от несанкционированного доступа и утечки по техническим каналам на соответствие требованиям по безопасности информации Методы защиты информации от несанкционированного доступа и утечки по техническим каналам Принципы формирования и реализации политики безопасности информации в автоматизированных системах		
Разработка архитектуры системы защиты информации автоматизированной системы	Проведение оценки показателей качества и эффективности работы вычислительных систем, программных и программно-аппаратных средств, используемых для построения систем защиты информации в автоматизированных системах Проведение технико-экономической оценки целесообразности создания системы защиты информации автоматизированной системы Определение порядка обработки информации в ав-	Определять комплекс мер для обеспечения безопасности информационной в автоматизированных системах Выявлять уязвимости информационно-технологических ресурсов автоматизированных систем Разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем Проводить выбор программно-аппаратных средств обеспечения безопасности информации для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизирован-	Основные информационные технологии, используемые в автоматизированных системах Способы и средства защиты информации от несанкционированного доступа и утечки по техническим каналам и контроля эффективности защиты информации Основные средства и способы обеспечения безопасности информации, принципы построения систем защиты информации Программно-аппаратные средства обеспечения защиты информации автоматизированных систем Принципы построения средств защиты информации от несанкционированного доступа и утечки		

Трудовая функция в соответствии с профессиональным стандартом	Перечень профессиональных компетенций	Необходимые умения	Необходимые знания	Разделы программы, формирующие профессиональные компетенции	Форма проверки сформированности компетенции
	томатизированной системе Формирование разделов технических заданий на создание систем защиты информации автоматизированных систем Разработка проектной документации на системы защиты автоматизированных систем Оформление заявки на разработку системы защиты информации автоматизированной системы	ной системы Классифицировать и оценивать угрозы безопасности информации для автоматизированной системы Определять информационную инфраструктуру и информационные ресурсы автоматизированной системы, подлежащие защите Разрабатывать модели угроз безопасности информации и нарушителей в автоматизированных системах Определять эффективность применения средств информатизации	по техническим каналам Национальные, межгосударственные и международные стандарты в области защиты информации Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации Организационные меры по защите информации Методы тестирования и отладки, принципы организации документирования разработки, процесса сопровождения программного обеспечения		
Моделирование защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации	Разработка аналитических и компьютерных моделей автоматизированных систем и подсистем безопасности автоматизированных систем Исследование аналитических и компьютерных моделей автоматизированных систем и подсистем безопасности автоматизированных систем Разработка модели угроз безопасности информации и нарушителей в автоматизированных системах Исследование программных, архитектурно-технических и схемотехнических решений компонентов автоматизированных систем с целью выявления потенциальных уязвимо-	Выполнять сбор, обработку, анализ и систематизацию научно-технической информации в области защиты информации Разрабатывать и исследовать математические модели конкретных явлений и процессов для решения расчетных и исследовательских задач Применять математические модели при проектировании систем защиты информации автоматизированных систем Проектировать и реализовывать политику безопасности вычислительных сетей Анализировать основные характеристики и возможности телекоммуникационных систем по передаче информации	Методы и технологии проектирования, моделирования, исследования систем защиты информации автоматизированных систем Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах Основные меры по защите информации в автоматизированных системах Национальные, межгосударственные и международные стандарты в области защиты информации Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах Принципы построения средств		

Трудовая функция в соответствии с профессиональным стандартом	Перечень профессиональных компетенций	Необходимые умения	Необходимые знания	Разделы программы, формирующие профессиональные компетенции	Форма проверки сформированности компетенции
	стей безопасности информации в автоматизированных системах Анализ информационной инфраструктуры и безопасности информации автоматизированных систем Разработка предложений по совершенствованию системы управления информационной безопасностью автоматизированных систем		защиты информации от несанкционированного доступа и утечки по техническим каналам Принципы построения и функционирования систем и сетей передачи информации		

3. Содержание программы

Раздел 1. Основы информационной безопасности.

Тема 1.1. Теория информационной безопасности и методология защиты информации.

Тема 1.2. Правовое, нормативное и методическое регулирование деятельности в области защиты информации.

Тема 1.3. Правовые основы организации защиты государственной тайны, задачи органов защиты государственной тайны.

Раздел 2. Техническая защита информации.

Тема 2.1. Угрозы и уязвимости автоматизированных информационных систем.

Тема 2.2. Классификация технических каналов утечки информации.

Тема 2.3. Виды уязвимостей автоматизированных информационных систем.

Тема 2.4. Оценка уровня защищённости информационных систем.

Тема 2.5. Методы и средства технической защиты информации.

Раздел 3. Защита информации с использованием шифровальных (криптографических) средств

Тема 3.1. Криптографические методы защиты информации.

Тема 3.2. Обеспечение применения электронной подписи и инфраструктуры открытого ключа с использованием сертифицированных средств.

Раздел 4. Комплексная защита объектов информатизации

Тема 4.1. Информационная безопасность автоматизированных систем.

Тема 4.2. Обеспечение безопасности персональных данных, обрабатываемых в информационных системах (ИСПДн).

Тема 4.3. Особенности защиты информации, составляющей коммерческую тайну компании.

Тема 4.4. Обеспечение безопасности объектов критической информационной инфраструктуры

Раздел 5. Управление информационной безопасностью.

Тема 5.1. Управление информационной безопасностью.

Тема 5.2. Организация конфиденциального делопроизводства.

Тема 5.3. Аудит информационной безопасности.

Тема 5.4. Экономика защиты информации

Раздел 6. Аттестация объектов информатизации по требованиям безопасности информации

Тема 6. Подготовка документов для аттестации объектов информатизации по требованиям безопасности информации.

Тема 7. Методики обоснования выбора средств технической и криптографической защиты информации.

Тема 8. Особенности эксплуатации технических средств защиты информации.

Тема 9. Применение шифровальных (криптографических) средства защиты информации различных производителей.

Тема 10. Выбор, установка, настройка и эксплуатация средств антивирусной защиты.

Тема 11. Программные средства анализа рисков информационной безопасности.

4. Учебный план программы

№	Наименование раздела	Кол-во	Очная форма	Заочная форма	Форма

п/п		часов, всего	Лекции, часов	Практические занятия, часов	Самостоятельная работа, часов	Лекции, часов	Практические занятия, часов	Самостоятельная работа, часов	контроля
1	**Раздел 1. Основы информационной безопасности.**	**72**	**28**	**32**	**12**	**6**	**10**	**56**	**реферат**
2	Тема 1.1. Теория информационной безопасности и методология защиты информации.	18	6	8	4	2	2	14	
3	Тема 1.2. Правовое, нормативное и методическое регулирование деятельности в области защиты информации.	36	16	16	4	2	6	28	
4	Тема 1.3. Правовые основы организации защиты государственной тайны, задачи органов защиты государственной тайны.	18	6	8	4	2	2	14	
5	**Раздел 2. Техническая защита информации.**	**108**	**46**	**48**	**12**	**14**	**16**	**78**	**реферат**
6	Тема 2.1. Угрозы и уязвимости автоматизированных информационных систем.	10	4	4	2	2	2	6	
7	Тема 2.2. Классификация технических каналов утечки информации.	10	4	4	2	2	2	6	
8	Тема 2.3. Виды уязвимостей автоматизированных информационных систем.	10	4	4	2	2	2	6	
9	Тема 2.4. Оценка уровня защищённости информационных систем.	32	14	14	4	4	4	24	
10	Тема 2.5. Методы и средства технической защиты информации.	46	20	22	4	4	6	36	
11	**Раздел 3. Защита информации с использованием шифровальных (криптографических) средств**	**108**	**50**	**50**	**8**	**16**	**16**	**76**	**реферат**
12	Тема 3.1. Криптографические методы защиты информации.	76	36	36	4	10	10	56	
13	Тема 3.2. Обеспечение применения электронной подписи и инфраструктуры открытого ключа с использованием сертифицированных средств.	32	14	14	4	6	6	20	
14	**Раздел 4. Комплексная защита объектов информатизации**	**72**	**32**	**32**	**8**	**8**	**8**	**56**	**реферат**
15	Тема 4.1. Информационная безопасность автоматизированных систем.	18	8	8	2	2	2	14	
16	Тема 4.2. Обеспечение безопасности персональных данных, обрабатываемых в информационных системах (ИСПДн).	18	8	8	2	2	2	14	

17	Тема 4.3. Особенности защиты информации, составляющей коммерческую тайну компании.	18	8	8	2	2	2	14	
18	Тема 4.4. Обеспечение безопасности объектов критической информационной инфраструктуры	18	8	8	2	2	2	14	
19	**Раздел 5. Управление информационной безопасностью.**	**72**	**32**	**32**	**8**	**8**	**8**	**56**	**реферат**
20	Тема 5.1. Управление информационной безопасностью.	18	8	8	2	2	2	14	
21	Тема 5.2. Организация конфиденциального делопроизводства.	18	8	8	2	2	2	14	
22	Тема 5.3. Аудит информационной безопасности.	18	8	8	2	2	2	14	
23	Тема 5.4. Экономика защиты информации	18	8	8	2	2	2	14	
24	**Раздел 6. Аттестация объектов информатизации по требованиям безопасности информации**	**72**	**24**	**34**	**14**	**12**	**6**	**54**	**реферат**
25	Тема 6.1. Подготовка документов для аттестации объектов информатизации по требованиям безопасности информации.	16	6	8	2	2	2	12	
26	Тема 6.2. Методики обоснования выбора средств технической и криптографической защиты информации.	8	2	4	2	2	-	6	
27	Тема 6.3. Особенности эксплуатации технических средств защиты информации.	16	6	8	2	2	2	12	
28	Тема 6.4. Применение шифровальных (криптографических) средства защиты информации различных производителей.	16	6	8	4	2	2	12	
29	Тема 6.5. Выбор, установка, настройка и эксплуатация средств антивирусной защиты.	8	2	4	2	2	-	6	
30	Тема 6.6. Программные средства анализа рисков информационной безопасности.	8	2	4	2	2	-	6	
31	**Итоговая аттестация**	**16**							**экзамен**

5. Организационно-педагогические условия реализации программы

Для всех видов аудиторных занятий продолжительность академического часа составляет 45 минут. Допускается проведение сдвоенных занятий (2 академических часа продолжительностью 90 минут).

Для реализации задач обучения предусматриваются различные виды учебных занятий и форм контроля.

Основными видами учебных занятий являются:

- лекция;
- семинарское занятие;
- практическое занятие;
- самостоятельная работа.

Дополнительно к основным возможно использование следующих видов учебных занятий: консультация, тренинг, деловая игра, разбор конкретных примеров (кейс-стади), круглый стол.

Лекция является одним из видов учебных занятий, направленных, прежде всего, на теоретическую подготовку слушателей. Цель лекции – дать систематизированные основы знаний по учебной дисциплине, акцентировав внимание на наиболее сложных вопросах темы. Лекция должна стимулировать активную познавательную деятельность слушателей, способствовать формированию их творческого мышления.

Семинарское занятие проводится с целью углубления и закрепления знаний, полученных на лекции и в процессе самостоятельной работы над учебной литературой. Его организация должна обеспечивать обмен мнениями, живое, творческое обсуждение учебного материала, дискуссии по рассматриваемым вопросам, максимальную мыслительную активность слушателей на протяжении всего занятия. Семинарское занятие может содержать элементы практического занятия (решение задач и т.п.). Семинарские занятия проводятся по темам, требующим более углубленного тематического изучения.

Практическое занятие проводится с целью приобретения, отработки и закрепления слушателями практических умений и навыков. Главным содержанием практического занятия является практическая работа каждого слушателя. В ходе практического занятия слушатели находят ответы на наиболее сложные вопросы, моделируют различные ситуации, которые могут возникнуть в ходе применения законодательства Российской Федерации на практике, анализируют поведение различных субъектов на примере конкретных задач. В течение практического занятия преподаватель осуществляет коммуникативную и информационную поддержку слушателей, как в текущем режиме, так и в режиме «он-лайн» при использовании информационных технологий обучения.

Деловые игры могут проводиться по комплексным проблемам, возникающим в сфере профессиональной деятельности слушателей, с целью приобретения и закрепления у слушателей навыков практической деятельности путем моделирования (воспроизведения) профессиональной деятельности. В течение практического занятия и деловой игры (около двух – четырех аудиторных часов) преподаватель осуществляет коммуникативную и информационную поддержку слушателей.

Самостоятельная работа слушателей направлена на изучение, углубление и закрепление знаний, полученных на лекциях и других занятиях, выработку навыков самостоятельного приобретения знаний. Самостоятельная работа проводится в виде решения слушателями от 10 до 20 практических ситуаций, связанных с закупками продукции для государственных и муниципальных нужд.

Консультация является одной из форм учебных занятий, которая обеспечивает помощь слушателям в самостоятельном освоении учебного материала. Консультации носят как индивидуальный, так и групповой характер.

Тренинг представляет собой одну из форм учебных занятий, направленную на получение знаний, приобретение навыков. На тренинге слушатели развивают умения, приобретают навыки и получают знания о том, как лучше и эффективно разбираться в

вопросе, которому посвящен тренинг. В ходе проведения тренинга отводится время для ответов на вопросы слушателей преподавателем.

Разбор конкретных примеров (кейс-стади) – вид учебного занятия, суть которого заключается в самостоятельной деятельности слушателей в искусственно созданной профессиональной среде. Данный метод представляет собой активное обучение на основе реальных ситуаций, направленное на освоение конкретных знаний и умений, развитие общего интеллектуального и коммуникативного потенциала слушателей.

Круглый стол позволяет слушателям обменяться опытом и знаниями, систематизировать точки зрения по наиболее проблемным вопросам практической деятельности слушателей.

6. Итоговая аттестация слушателей

Итоговый контроль (итоговая аттестация) позволяет проверить уровень усвоения слушателем учебного материала (изучение теоретических основ, приобретение профессиональных навыков, формирование профессиональной компетентности).

При проведении итоговой аттестации осуществляется оценка следующих профессиональных компетенций слушателей, сформированных в ходе обучения:

– Обслуживание систем защиты информации в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости

– Обеспечение защиты информации в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости, в процессе их эксплуатации

– Разработка систем защиты информации автоматизированных систем, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости

– Формирование требований к защите информации в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости

До участия в итоговой аттестации допускаются слушатели, освоившие образовательную программу.

Итоговый контроль (итоговая аттестация) проводится с помощью экзамена в форме тестирования.

Вопросы для тестирования охватывают различные дисциплины и темы Программы и включают в себя не менее трех вопросов по каждой из предусмотренных тем. При проведении зачета предусмотрено не менее 2 вариантов тестов. Тест может содержать от 15 до 20 вопросов, на каждый вопрос предусмотрено 3-4 варианта ответа. Не менее трети заданий теста носят практико-ориентированный характер. Регламент времени на заполнение теста до 2 академических часов.

Перечень вопросов составляется непосредственно перед итоговым контролем.

Критерии оценивания знаний слушателей.

Зачет предусматривает балльную систему оценивания:

- менее 51% правильных ответов – «неудовлетворительно»;
- от 51% до 70% правильных ответов – «удовлетворительно»;

- от 71% до 85% правильных ответов – «хорошо»;

- 86% и более правильных ответов – «отлично».

В случае неудовлетворительного результата итоговой аттестации допускается повторное прохождение итогового контроля с заменой варианта тестового материала.

Слушателям, успешно прошедшим итоговую аттестацию, выдаются удостоверения о повышении квалификации.

7. Перечень рекомендуемой литературы

а) нормативно-правовые акты:

Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации»

Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»

Федеральный закон от 07.07.2003 г. № 126-ФЗ «О связи»

Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании»

Федеральный закон от 04 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне»

Федеральный закон от 26 июня 2008 г. № 102-ФЗ «Об обеспечении единства измерений»

Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»

Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю»

Указ Президента Российской Федерации от 06 марта 1997 г. №188 «Об утверждении перечня сведений конфиденциального характера»

Доктрина информационной безопасности Российской Федерации. (утверждена Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895)

Постановление Правительства Российской Федерации от 26 июня 1995 г. № 608 «Об утверждении Положения о сертификации средств защиты информации»

Постановление Правительства Российской Федерации от 26 июня 1995 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

Постановление Правительства Российской Федерации от 3 февраля 2012 г. № 79 «Об утверждении Положения о лицензировании деятельности по технической защите конфиденциальной информации»

Постановление Правительства Российской Федерации от 02 марта 2012 г. №171 «Об утверждении Положения о лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации»

Постановление Правительства Российской Федерации от 03 ноября 1994 г. №1233 «Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти»

б) основная литература:

Семкин С.Н., СемкинА.Н.Основы информационной безопасности объектов обработки информации, 2000 г.

В.В. Домарев. Безопасность информационных технологий. Системный подход, 2004 г.

в) дополнительная литература:

Б. Шнайер. Секреты и ложь. Безопасность данных в цифровом мире, 2003 г.

Д. Скляров. Искусство защиты и взлома информации, 2004 г.

С.С. Корт. Теоретические основы защиты информации, 2004 г.

С.Н. Семкин и др. Основы организационного обеспечения информационной безопасности объектов информатизации, 2005 г.

В.В. Домарев. Защита информации и безопасность компьютерных систем, 1999 г.

В.В. Мельников. Безопасность информации в автоматизированных системах, 2003 г.

А.Ю. Щеглов. Защита компьютерной информации от несанкционированного доступа, 2004 г.

Т.Л. Партыка, Попов И.И. Информационная безопасность, 2004 г.

В.И. Ярочкин. Информационная безопасность. Учебник для вузов, 2004 г.

Т.Н. Устинов. Основы информационной безопасности систем и сетей передачи данных, 2000г.

В.А. Галатенко. Основы информационной безопасности. Курс лекций, 2004 г.

Теоретические основы компьютерной безопасности. Учебное пособие для вузов, 2000 г.

Соколов А.В., Степанюк О.М. Шпионские штучки. Методы информационной защиты объектов и компьютерных систем, 2000 г.

А.В. Петраков. Основы практической защиты информации. Учебное пособие, 2005г.

А.А. Губенков, В.Б. Байбурин. Информационная безопасность, Учебное пособие, 2005г.

С.В. Лебедь. Межсетевое экранирование. Теория и практика защиты внешнего периметра, 2002г.

В.Г. Проскурин, С.В. Крутов, И.В. Мацкевич. Защита в операционных системах, 2000г.

А.А. Снытников. Лицензирование и сертификация в области ЗИ, 2003г

Скотт Бармен. Разработка правил информационной безопасности, 2002г.

А.В. Ильичев. Начала системной безопасности, 2003г.

Г.Ф. Конахович. Защита информации в телекоммуникационных системах, 2005г.

Научно-практический сборник. Технические средства защиты информации, 2002г.

Вильям Столлинг. Основы защиты сетей. Приложения и стандарты, 2002г.

А.А. Соколов, О.М. Степанюк. Защита от компьютерного терроризма, 2002г.

В. Зима, А. Молдовян. Безопасность глобальных сетевых технологий, 2003г.

П. Девянин. Анализ безопасности управления доступом и информационными потоками в компьютерных системах, 2006г.

А.А. Садердинов, В.А. Трайнев и др. Учебное пособие. Информационная безопасность предприятия, 2006г.

Стивен Норткат, Мери Купер и др. Анализ типовых нарушений безопасности в сетях, 2001г.

Н.А. Гайдамакин. Разграничение доступа к информации в компьютерных системах, 2003г.

В.Я. Асанович, Т.Г. Маныпин. Информационная безопасность: анализ и прогноз информационного воздействия, 2006г.

Ю.К. Меньшаков. Защита объектов и информации от технических средств разведки, 2002г.

В.А. Конявский, С.В. Лопаткин. Компьютерная преступность, том 1, 2006г.

С.А. Запечников, И.Г. Милославская. Учебник Информационная безопасность открытых систем, том 1, 2006г.

А.А. Малюк, Учебное пособие. Информационная безопасность: концептуальные и методологические основы защиты информации, 2004г.

А.Н. Прохода. Обеспечение Интернет-безопасности, Учебное пособие, 2007г.

Учебное пособие. Защита информации в системах мобильной связи, 2006г.

А.А. Малюк. Введение в защиту информации в автоматизированных системах, 2005г.

Е.Б. Белов, В.П. Лось. Учебное пособие. Основы информационной безопасности, 2006г.

С.В. Запечников и др. Основы построения виртуальных частных сетей, 2003г.

г) базы данных, информационно-справочные и поисковые системы: Информационные правовые системы «Консультант Плюс» и «Гарант»;

8. Фонд оценочных средств

Тестовые вопросы

1. Выберите наиболее подходящее определение информации:

a) сведения о лицах, предметах;

b) сведения о лицах, предметах, фактах, событиях;

c) сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;

d) сведения о лицах независимо от формы их представления;

2. Информационная система – это …

a) набор программных и технических средств;

b) упорядоченную совокупность документов, информационных технологий и программно - аппаратных средств, реализующих информационные процессы;

c) упорядоченная совокупность документов, относящихся к определенной области;

d) набор программных средств, относящихся к одной задаче;

3. Информационными ресурсами называют:

a) документы (массивы документов), существующие в составе информационных систем;

b) документы (массивы документов), существующие отдельно или в составе информационных систем;

c) документы (массивы документов), существующие отдельно от информационных систем;

d) все определения не верны;

4. Информацию по степени доступа разделяют на:

a) открытую и ограниченного доступа;

b) открытую;

c) закрытую;

d) тайную и ограниченную;

5. К информации ограниченного доступа относятся:

a) государственная тайна;

b) конфиденциальная информация;

c) персональные данные;

d) все ответы верны

6. Собственник информационных ресурсов, систем и технологий – это:

a) субъект с полномочиями владения указанными объектами;

b) субъект с полномочиями владения и пользования указанными объектами;

c) субъект с полномочиями владения, пользования и распоряжения указанными объектами;

d) Все ответы верны;

7. Информационная безопасность являются переводом на русский язык английского термина:

a) information security;

b) information system;

c) information currency;

d) information crypto;

8. Защитой информации называют:

a) деятельность по предотвращению утечки любой информации;

b) деятельность по предотвращению утечки защищаемой информации;

c) деятельность по предотвращению утечки доступной информации;

d) все ответы верны;

9. Под утечкой понимают:

a) неконтролируемое распространение защищаемой информации путём её разглашения или несанкционированного доступа к ней;

b) неконтролируемое распространение скрытой информации путём её разглашения или несанкционированного доступа к ней;

c) неконтролируемое распространение конфиденциальной информации путём её разглашения или несанкционированного доступа к ней;

d) все верно;

10. Под непреднамеренным воздействием на защищаемую информацию понимают:

a) воздействие на неё из-за ошибок пользователя, сбоя технических или программных средств, иных нецеленаправленных действий;

b) воздействие на неё из-за ошибок пользователя, сбоя технических средств;

c) воздействие на неё из-за ошибок пользователя, программных средств, иных нецеленаправленных действий;

d) все ответы верны;

11. Что не является характеристикой информации:

a) статичность;

b) тип доступа;

c) время отклика;
d) стоимость создания;
12. Способность информации изменяться в процессе использования – это:
a) статичность;
b) тип доступа;
c) время жизни;
d) стоимость создания;
13. Промежуток времени, пока информация актуальна – это:
a) статичность;
b) тип доступа;
c) время жизни;
d) стоимость создания;
14. По оценке экспертов самым привлекательным сектором российской экономики для преступников является:
a) финансовая система;
b) кредитно-финансовая система;
c) кредитная система;
d) нет верного ответа ;
15. Какая стоимость будет наиболее велика для пластиковой карты?
a) стоимость создания;
b) стоимость потери конфиденциальности;
c) стоимость скрытого нарушения целостности;
d) стоимость утраты;
16. К наиболее распространённым правонарушениям в сети Internet не относится:
a) мошенническая деятельность;
b) перлюстрация частной переписки;
c) нарушение авторских и смежных прав;
d) нелегальное получение товаров и услуг;
17. Что не относится к задачам информационной безопасности:
a) целостность и секретность;
b) электронная подпись и датирование;
c) устойчивость связи и определение трафика;
d) неотказуемость и анонимность;
18. К методам обеспечения информационной безопасности не относятся:
a) корпоративные;
b) административные;
c) правовые;
d) технические;
19. Какие методы не относятся к обеспечению информационной безопасности:
a) принуждение и побуждение;
b) управление доступом и регламентация;
c) маскировка и препятствие;
d) скрытый доступ и копирование сообщений;
20. Методы защиты информации можно разбить:
a) на три большие группы;
b) на две большие группы;

c) на четыре большие группы;

d) на пять больших групп;

21. Методы, не имеющие математического обоснования стойкости, часто называют методами:

a) С чёрным ящиком;

b) С белым квадратом;

c) С желтым кругом;

d) Нет верного ответа;

22. Методы, функционирующие по принципу "черного ящика", называют

a) Security Through Obscurity;

b) System Through Obscurity;

c) Security Through;

d) System Obscurity;

23. Метод физического преграждения пути злоумышленнику к информации:

a) управление доступом;

b) маскировка;

c) принуждение;

d) побуждение;

24. Метод защиты информации путем ее криптографического преобразования:

a) Принуждение;

b) Побуждение;

c) Маскировка;

d) управление доступом;

25. Комплексное понятие, обозначающее совокупность методов и средств, предназначенных для ограничения доступа к ресурсам:

a) Уполномочивание;

b) Контроль доступа;

c) Сертификация;

d) Нет верного ответа;

26. Основными характеристиками защищаемой информации являются:

a) конфиденциальность, целостность и статичность;

b) конфиденциальность, целостность и доступность;

c) аутентификация, целостность и доступность;

d) аутентификация, статичность и время создания;

27. Известность содержания информации только имеющим соответствующие полномочия субъектам – это:

a) Целостность;

b) Статичность;

c) Конфиденциальность;

d) Аутентификация;

28. Неизменность информации в условиях её случайного и (или) преднамеренного искажения и разрушения – это:

a) Целостность;

b) Конфиденциальность;

c) Доступность;

d) Идентификация;

29. Возможность получения информации или информационной услуги за приемлемое время – это:

a) конфиденциальность;

b) целостность;

c) доступность;

d) статичность;

30. Потенциально возможное событие, действие, процесс или явление, которое может привести к изменению функционирования компьютерной системы:

a) уязвимость;

b) атака;

c) угроза;

d) нет верного ответа;

31. Возможность возникновения на каком-либо этапе жизненного цикла компьютерной системы такого её состояния, при котором создаются условия для реализации угроз безопасности информации - это:

a) атака;

b) угроза;

c) уязвимость;

d) статичность;

32. Действия, предпринимаемые злоумышленником, которые заключаются в поиске и использовании уязвимостей информации – это:

a) статичность;

b) атака;

c) угроза;

d) изъян;

33. Классификацию угроз ИБ можно выполнить по нескольким критериям:

a) по аспекту информационной безопасности;

b) по компонентам информационной системы;

c) по способу осуществления;

d) все ответы верны;

34. Конфиденциальная информация может быть разделена на:

a) предметную и служебную;

b) служебную и закрытую;

c) предметную и открытую;

d) открытую и закрытую;

35. Целостность информации может быть разделена на:

a) статическую и динамическую;

b) статическую и служебную;

c) служебную и динамическую;

d) все верно;

36. Примером нарушения статической целостности не является:

a) ввод неверных данных;

b) несанкционированное изменение данных;

c) изменение программного модуля вирусом;

d) внесение дополнительных пакетов в сетевой трафик;

37. Примером нарушения динамической целостности не является:

a) нарушение атомарности транзакций;
b) внесение дополнительных пакетов в сетевой трафик;
c) несанкционированное изменение данных;
d) дублирование данных;
38. Угроза отказа служб может быть разбита на следующие типы:
a) отказ пользователей;
b) внутренний отказ информационной системы;
c) отказ поддерживающей инфраструктуры;
d) все ответы верны;
39. Что не относится к внутреннему отказу ИС:
a) ошибки при переконфигурировании системы;
b) отказы программного и аппаратного обеспечения;
c) разрушение данных;
d) нарушение работы систем связи;
40. Что не относится к отказу служб:
a) нарушение работы систем связи;
b) разрушение и повреждение помещений;
c) нарушение работы электропитания;
d) разрушение данных;
41. Нарушители классифицируются по одному из следующих критериев:
a) уровень профессиональной подготовки противника;
b) тип доступа противника к системе;
c) способы атаки;
d) все ответы верны;
42. Высококвалифицированный специалист, стремящейся обойти защиту компьютерной системы:
a) Крякер;
b) Хаб;
c) Хакер;
d)Юзер;
43. Наибольшую угрозу ИС составляют:
a) Юзер;
b) Агент;
c) Хакер;
d) Крякер;
44. На сколько больших классов делятся каналы утечки информации:
a) Два;
b) Три;
c) Четыре;
d) Пять;
45. Что не относится к косвенным каналам утечки информации:
a) дистанционное видеонаблюдение;
b) использование подслушивающих устройств;
c) перехват побочных электромагнитных излучений и наводок;
d) хищение носителей информации;
46. Какая угроза отказа служб устраняется административноправовыми метода-

ми:

a) отказ пользователей;

b) отказ программного обеспечения;

c) нарушение работ систем связи;

d) разрушение и повреждение помещений

47. К каналам, предполагающим изменение элементов информационной структуры относится:

a) намеренное копирование файлов и носителей информации;

b) маскировка под других пользователей, путём похищение идентифицирующей их информации;

c) хищение носителей информации;

d) незаконное подключение специальной регистрирующей аппаратуры к устройствам связи.

48. Что относится к каналам, не требующим изменение элементов ИС

a. намеренное копирование файлов и носителей информации;

b. незаконное подключение специальной регистрирующей аппаратуры;

c. злоумышленное изменение программ;

d. злоумышленный вывод из строя средств защиты информации;

49. Какая направленность атак неверно сформулирована?

a) атаки на уровне операционной системы;

b) атаки на уровне системного администратора;

c) атаки на уровне сетевого программного обеспечения;

d) атаки на уровне систем управления базами данных.

50. К какому типу атак относится прослушивание передаваемых сообщений:

a) Пассивная атака;

b) Модификация потока данных;

c) Повторное использование;

d) Отказ в обслуживании;

51. АИС – это:

a) автоматизированная информационная среда;

b) автоматизированная информационная схема;

c) автоматизированная информационная система;

d) автоматизированная информационная структура;

52. Принципы обеспечения информационной безопасности:

a) системность, комплексность, непрерывность;

b) статичность, комплексность, доступность;

c) комплексность, целостность, доступность;

d) целостность, системность, открытость;

53. Выбор методов и средств, направленных на противодействие комплексу угроз – это:

a) Целостность;

b) Системность;

c) Комплексность;

d) Непрерывность;

54. Возможность изменения применяемых средств ИС – это:

a) Комплексность;

b) Гибкость;

c) Непрерывность;

d) Целостность;

55. Самая распространенная формальная модель доступа к данным:

a) Мандатная;

b) Дискреционная;

c) модель Биба;

d) модель Кларка;

56. В дискреционной модели отношения субъекты - объекты представлены в виде:

a) Таблиц;

b) Матриц;

c) Схем;

d) все верно;

57. В какой модели доступа каждому объекту системы присвоена метка секретности:

a) модель Кларка;

b) дискреционная;

c) мандатная;

d) модель Биба;

58. Центральный элемент системы защиты, который идентифицирует субъекты, объекты и параметры запрашиваемого доступа субъектов к объектам:

a) Монитор безопасности

b) сканер;

c) модем безопасности;

d) шина безопасности;

59. К административному уровню информационной безопасности относятся действия общего характера, предпринимаемые:

a) руководством организации

b) Персоналом организации

c) Пользователями

d) Нет верного ответа

60. Из скольких уровней детализации состоит политика безопасности ИС:

a) Трех

b) Четырех

c) Двух

d) Пяти

61. Политика безопасности верхнего уровня, затрагивающая все организацию в целом, включает в себя:

a) решение сформировать или изменить комплексную программу обеспечения информационной безопасности;

b) формулирование целей организации в области информационной безопасности, определение общих направлений в достижении данных целей;

c) обеспечение нормативной базы для соблюдения законов и правил;

d) все ответы верны;

62. Самая распространенная сетевая ос:

a) Novell Netware;

b) MS Windows;

c) UNIX;

d) Os/2;

63. Наиболее распространёнными методами несанкционированного доступа в операционной системе Unix является:

a) Позволяющие несанкционированно запустить исполняемый код;

b) Позволяющие обойти установленные разграничения прав доступа;

c) Троянские программы;

d) Позволяющие осуществить несанкционированные операции чтения/записи файловых и других объектов;

64. Наиболее распространёнными методами несанкционированного доступа в операционной системе Windows является:

a) Позволяющие несанкционированно запустить исполняемый код;

b) Позволяющие обойти установленные разграничения прав доступа;

c) Троянские программы;

d) Позволяющие осуществить несанкционированные операции чтения/записи файловых и других объектов.

65. Что не относится к недостаткам ОС Windows?

a) невозможно встроенными средствами гарантированно удалять остаточную информацию;

b) не обеспечивается регистрация выдачи документов на "твёрдую копию", а также некоторые другие требования к регистрации событий;

c) невозможно в общем случае обеспечить замкнутость (или целостность) программной среды;

d) невозможно встроенными средствами обеспечить полноту системы

66. Из скольких уровней состоит правовое обеспечение информационной безопасности:

a) двух уровней;

b) трех уровней;

c) четырех уровней;

d) пяти уровней;

67. Что из перечисленного не входит в первый уровень правового обеспечения информационной безопасности:

a) Конституция РФ (ст. 23, право на тайну переписки);

b) Гражданский кодекс РФ (ст. 139, возмещение убытков от утечек);

c) Федеральный закон "О государственной тайне";

d) постановления Правительства РФ;

68. Что из перечисленного не входит во второй уровень правового обеспечения информационной безопасности:

a) указы Президента РФ;

b) постановления Правительства РФ;

c) Уголовный кодекс РФ (ст. 272-274, неправомерный доступ, распространение вирусов, нарушение правил эксплуатации);

d) постановления пленумов Верховного Суда РФ;

69. Структурные элементы национальной безопасности:

a) Политическая;
b) Экономическая;
c) Военная;
d) все ответы верны;
70. Как на английском пишется термин уязвимость:
a) Vulnerability;
b) Secure;
c) Source;
d) Vain;
71. Систему национальной безопасности образует:
a) органы законодательной, исполнительной и судебной властей;
b) государственные, общественные и иные организации и объединения;
c) граждане, принимающие участие в обеспечении безопасности в соответствии с законом;
d) все ответы верны;
72. В каком году утверждена Доктрина информационной безопасности Российской Федерации:
a) 1998;
b) 2000;
c) 2002;
d) 2004;
73. Что не относится к основным принципам обеспечения национальной безопасности:
a) законность;
b) соблюдение баланса жизненно важных интересов личности, общества и государства;
c) взаимная ответственность личности, общества и государства по обеспечению безопасности;
d) системность;
74. К правовым методам обеспечения информационной безопасности относят:
a) разработка современных методов и средств защиты информации;
b) определение ответственности физических и юридических лиц;
c) усиление контроля за развитием информационного рынка России;
d) повышение степени защищенности законных интересов граждан;
75. Когда был принят Федеральный закон "Об информации, информатизации и защите информации:
a) 2004;
b) 1995;
c) 2008;
d) 1998;
76. От какого арабского слова происходит Термин шифр:
a) Символ;
b) Пароль;
c) Цифра;
d) Код;
77. Как переводится слово криптография:

a) Тайнопись;
b) Рукопись;
c) Алгоритм;
d) Пароль;
78. Чем занимается криптография:
a) составлением алгоритмов шифрования информации;
b) составлением алгоритмов передачи информации;
c) составлением прикладных программ;
d) составлением инструментальных программ;
79. Исследование криптографических алгоритмов с целью оценки их стойкости и поиска слабых мест называется:
a) Криптографией;
b) Криплоанализом;
c) Шифрованием;
d) Кодированием;
80. Процесс преобразования открытого текста в шифртекст называется:
a) Enciphering;
b) Deciphering;
c) Cryptanalysis;
d) Algorithm;
81. Процесс преобразования шифрованного текста в исходный называется:
a) Enciphering ;
e) Algorithm;
f) Deciphering;
g) Cryptanalysis;
82. Элемент позволяющий выбрать одно конкретное преобразование из множества преобразований – это:
a) Ключ;
b) Пароль;
c) Код;
d) Шифр;
83. Раскрытие ключа шифрования без привлечения методов криптоанализа называется:
a) Компрометацией;
b) Криптоанализом;
c) Шифрованием;
d) Криптографией;
84. Какая из перечисленных задач не относится к задачам криптографии:
a) Секретность;
b) Целостность;
c) Аутентификация;
d) Системность;
85. Выберите два основных типа криптографических алгоритмов:
a) Симметричные и асимметричные;
b) Симметричные и циклические;
c) Структурные и циклические;

d) Блочные и асимметричные;

86. В каких алгоритмах ключ расшифрования совпадает с ключом зашифрования:

a) Блочных;

b) Циклических;

c) Симметричных;

d) Асимметричных;

87. В современных шифрах применяется принцип:

a) Керкхоффса;

b) Хофмана;

c) Шенона;

d) Эль гаммеля;

88. Криптографические устройства псевдослучайных чисел – это:

a) Стартер;

b) Генератор;

c) Шина;

d) Магистраль;

89. Последовательность шагов, которые предпринимают две или большое количество сторон для совместного решения задачи – это:

a) Аудит;

b) Протокол;

c) Аутентификация;

d) Идентификация;

90. К основным криптографическим протоколам не относят:

a) обмен ключами;

b) аутентификацию;

c) цифровую подпись;

d) датирование;

91. Что не относится к Сервисам безопасности:

a) идентификация и аутентификация;

b) Шифрование;

c) инверсия паролей;

d) контроль целостности;

92. Что не относится к разделам криптографии:

a) Симметричные криптосистемы;

b) Системы электронной подписи;

c) Управление передачей данных;

d) Управление ключами;

93. Какого шифра не сушествует:

a) Шифр Цезаря;

b) Шифр Кардано;

c) Шифр Трисемуса;

d) Шифр Хартли;

94. Набор простых логических правил, легко применимых на практике и позволяющих выявить отдельные изъяны криптографических протоколов:

a) Бан – логика;

b) Пан – логика;

c) Ран – логика;
d) Фан – логика;
95. Процесс подтверждения подлинности пользователя – это:
a) Идентификация;
b) Аутентификация;
c) Методология;
d) Интеграция;
96. Каким шифром является DES
a) Симметричным;
b) Асимметричным;
c) Структурным;
d) Каскадным;
97. Сколько ключей надо перебрать для взлома алгоритма шифрования DES ,который имеет рабочую длину 56 бит:
a) 2 56
b) 2 5
c) 562
d) 2 6
98. Как по-другому называют ключ шифрования:
a) Сменный шифр;
b) Сменный элемент;
c) Сменная буква;
d) Сменный символ;
99. Какого типа электронной подписи не существует:
a) DSA;
b) RSA;
c) DTS;
d) CPO;
100. Каким шифром является RSA:
a) Симметрицным;
b) Асимметричным;
c) Структурным;
d) Компазиционным;
101. Что не относится к основным аппаратным средствам защиты информации:
a) пластиковые карты;
b) электронные замки;
c) магнитные карты;
d) видео карты;
102. Какой из перечисленных уровней предусматривает логическую защиту информации:
a) Внешний уровень, охватывающий всю территорию расположения ВС;
b) Уровень отдельных сооружений или помещений;
c) уровень технологических процессов хранения, обработки и передачи информации;
d) Уровень компонентов ВС;
103. Какой из перечисленных классов не относится к классам защиты информа-

ции:

a) Физический;

b) Программно-аппаратный;

c) Технологический;

d) Организационный;

104. Какие из перечисленных средств применяются для физической защиты информации:

a) лазерные и оптические системы;

b) механические и электронные замки;

c) телевизионные системы наблюдения;

d) все верно;

105. Для регистрации событий подключения к ВС ведется:

a) Видеонаблюдение;

b) База данных;

c) Аудит;

d) Протокол;

106. Защита от НСД со стороны пользователей в современных системах в основном реализуется:

a) парольная защита;

b) аутентификация;

c) идентификация;

d) все верно;

107. Какой из перечисленных способов не используется для аутентификации пользователя:

a) запрос секретного пароля;

b) применение микропроцессорных карточек;

c) биометрические средства;

d) Датирование;

108. Сложный вариант электронного ключа – это:

a) Пластиковая карта;

b) Жетон;

c) Шифр;

d) Подпись;

109. Из множества существующих средств аутентификации, наиболее надежными являются:

a) средства распознавания;

b) биометрические средства;

c) электронный ключ;

d) микропроцессорные карточки;

110. Что не относится к биометрическим средствам:

a) Отпечаток пальца;

b) Сетчатка глаза;

c) Голос;

d) Имя;

111. Сбор и накопление информации о событиях ИС – это:

a) Протоколирование;

b) Аудит;
c) журнал данных;
d) Синтез;
112. Анализ накопленной информации, проводимый оперативно или периодически:
a) Синтез;
b) Протоколирование;
c) Аудит;
d) Нет правильного варианта;
113. При протоколировании рекомендуют записывать следующую информацию:
a) Дата и время события;
b) Результат события;
c) Источник запроса;
d) Все верно;
114. Исполняемый или интерпретируемый программный код, обладающий свойством несанкционированного распространения и самовоспроизведения:
a) паразит;
b) вирус;
c) призрак;
d) нет верного ответа;
115. По особенностям реализуемого алгоритма вирусы делятся на:
a) Спутники, стелсы, паразиты, призраки;
b) стелсы, спутники, призраки, черви;
c) паразиты, призраки, черви, стелсы;
d) нет верного ответа;
116. Рекламная рассылка – это:
a) Спак;
b) Спам;
c) Спар;
d) Сапс;
117. Что необходимо иметь для проверки на вирус жесткого диска:
a) защищенную программу;
b)загрузочную программу;
c) файл с антивирусной программой;
d) антивирусную программу, установленную на компьютер;
118. Основными путями проникновения вирусов в компьютер являются:
a) Гибкие диски;
b) Компьютерные сети;
c) Больной пользователь;
d) Все верно;
119. Компьютерные вирусы:
a) возникают в связи со сбоями в аппаратных средствах компьютера;
b) пишутся людьми специально для нанесения ущерба;
c) зарождаются при работе неверно написанных программных продуктов;
d) являются следствием ошибок в операционной системе;
120. Загрузочные вирусы характеризуются тем, что:

a) поражают загрузочные сектора дисков;

b) поражают программы в начале их работы;

c) запускаются при загрузке компьютера;

d) изменяют весь код заражаемого файла

121. Может ли присутствовать компьютерный вирус на чистой дискете (на дискете отсутствуют файлы)?

a) Нет;

b) да, в области данных;

c) да, в области каталога;

d) да, в загрузочном секторе дискеты;

122. Вирус, у которого каждая следующая копия в заражённых объектах отличается от предыдущих – это:

a) Стелс;

b) Спутник;

c) Призрак;

d) Паразит;

123. Самые популярные антивирусные программы – это:

a) kaspersky, avg, panda;

b) avast, kaspersky, dr web;

c) McAfee, avg, panda;

d) kaspersky, avg, Symantec;

124. Какие программы относятся к антивирусникам:

a) kaspersky, avg, paint;

b) avp, dr web, avast;

c) avg, paint, McAfee;

d) avast, kaspersky, corel;

125. Когда появились первые антивирусные утилиты:

a) 1980;

b) 1982;

c) 1984;

d) 1986;

126. Совокупность взаимодействующих компонентов ИС и связей между ними - это:

a) Схема;

b) Система;

c) Структура;

d) Цикл;

127. Что не входит в нормативно- методическое обеспечение создания АС:

a) международные стандарты ISO;

b) стандарты Российской Федерации ГОСТ Р.;

c) стандарты организации-заказчика;

d) стандарты администрирования;

128. Как называется период времени, который начинается с момента принятия решения о необходимости создания АС и заканчивается в момент ее полного изъятия из эксплуатации:

a) ЖЦ АС;

b) ЖС АС;
c) ЖР АИ;
d) ЖМ ИС;

129. Совокупность функциональных и физических характеристик, установленных в технической документации и реализованных в программно-аппаратном комплексе – это

a) Конфигурация АС;
b) Структура АС;
c) Архитектура АС;
d) Нет верного ответа;

130. Совокупность свойств, которые характеризуют способность АС удовлетворять заданным требованиям:

a) Количество АС;
b) Качество АС;
c) Организация АС;
d) Все ответы верны;

131. Структура системы, определяющая последовательность выполнения и взаимосвязей целей и задач на протяжении ЖЦ:

a) План;
b) Модель;
c) Макет;
d) Схема;

132. Набор основных правил, определяющих организацию системы:

a) Конфигурация АС;
b) Структура АС;
c) Архитектура АС;
d) Нет верного ответа;

133. Под угрозой удаленного администрирования в компьютерной сети понимается угроза:

a) несанкционированного управления удаленным компьютером;
b) внедрения агрессивного программного кода в рамках активных объектов Web-страниц;
c) перехвата или подмены данных на путях транспортировки;
d) вмешательства в личную жизнь;

134. Наиболее эффективное средство для защиты от сетевых атак:

a) использование сетевых экранов или «firewall»
b. использование антивирусных программ
c. посещение только «надёжных» Интернет-узлов
d. использование только сертифицированных программ-броузеров при доступе к сети Интернет

135.Первым оценочным стандартом, получившим широкое распространение, стал стандарт Министерство обороны США:

a) Красная книга;
b) Оранжевая книга;
c) Синяя книга;
d) Желтая книга;

136.В каком году появился стандарт Министерство обороны США «Критерии оценки доверенных компьютерных систем»:

a) 1982;

b) 1983;

c) 1984;

d) 1985;

137. В стандарте Критерии оценки доверенных компьютерных систем» Степень доверия оценивается:

a) По двум критериям;

b) По трем критериям;

c) По четырем критериям;

d) Нет верного ответа;

138.Какого вида защиты нет в оранжевой книге:

a) Дискреционная защита;

b) Верифицированная защита;

c) Мандатная защита;

d) Максимальная защита;

139.Какой категории требований безопасности нет в «Оранжевой книге»:

a) политика безопасности;

b) подотчетность;

c) Корректность;

d) Статичность;

140. Как расшифровывается Стандарт ISO:

a) International Organization for System;

b) Information Organization for Standardization;

c) International Organization for Standardization;

d) International Organization for sertification;

141.Когда вышел стандарт ISO в области информационной безопасности:

a. 1998;

b. 1999;

c. 1997;

d. 2000;

142.Какой из этих уровней не рассматривают при формальном подходе к разработке ИС:

a) Цели;

b) Средства;

c) Реализация;

d) Финансы;

143.Как называется информационный документ, описывающий методику разработки защищенных систем:

a) Защищенные информационные системы;

b) Открытые информационные системы;

c) Скрытые информационные системы;

d) Доступные информационные системы;

144. Как переводится выражение Fair Information Practices:

a) Принцип честного использования информации;

b) Принцип скрытого использования информации;
c) Принцип закрытого использования информации;
d) Принципами открытого использования информации;
145.Какой из этих стандартов является одним из наиболее известных стандартов в области защиты информации:
a) information technology — Information security management;
b) information technology — Information system management;
c) information grafic — Information security management;
d) information technology — Information security office;
146.Стандарт для беспроводных локальных сетей – это:
a) Стандарт IEEE 801.11;
b) Стандарт IEEE 802.11;
c) Стандарт IEEE 802.12;
d) Стандарт IEEE 802.111;
147.Какой алгоритм придуман стандартом IEEE 802.11 для защиты WLAN:
a) Wep;
b) Web;
c) Wna;
d) Win;
148. Как переводится термин Wi-Fi
a) Wyb Fidelity;
b) Web Fidelity;
c) Wna Fidelity;
d) Wireless Fidelity;
149. Перспективный стандарт безопасных электронных транзакций в сети Интернет, предназначенный для организации электронной торговли через сеть Интернет – это:
a) Set;
b) Sid;
c) Ser;
d) Sis;
150.В каком году Гостехкомиссия (ГТК) при Президенте РФ опубликовала пять руководящих документов, посвященных вопросам защиты от несанкционированного доступа к информации:
a) 1990;
b) 1991;
c) 1992;
d) 1994;

9. Материально-техническое обеспечение

Для обеспечения дополнительно профессиональной программы используются специальные помещения, представляющие собой учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы и помещения для хранения и профилактического обслуживания учебного оборудования. Указанные помещения укомплектованы специализированной мебелью и техническими

средствами обучения, служащими для представления учебной информации большой аудитории.

Для освоения дисциплины (модуля) применяется специализированная многофункциональная аудитория:

Учебная аудитория для проведения занятий лекционного и семинарского типа: ПК, специализированная учебная мебель.

Учебная аудитория для проведения групповых и индивидуальных консультаций: ПК, специализированная учебная мебель.

Учебная аудитория для проведения текущего контроля и промежуточной аттестации: ПК, специализированная учебная мебель.

Помещение для самостоятельной работы с возможностью подключения к сети «Интернет»: ПК, специализированная учебная мебель.

Составитель: к.ф.-м.н., доцент Черняева С. Н.