Государственное образовательное автономное учреждение

высшего профессионального образования Курской области

«Курская академия государственной и муниципальной службы»

Кафедра философии, социально-правовых и естественнонаучных дисциплин

Дополнительная профессиональная программа рассмотрена на Межкафедральном учебно-методическом совете и утверждена к использованию в учебном процессе

Протокол № 2 от «12» декабря 2017 г.

Председатель \_\_\_\_\_\_\_\_\_\_\_\_\_И.В. Анциферова

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА

повышения квалификации

**«Комплексная защита информации и обеспечение безопасности персональных данных»**

|  |  |
| --- | --- |
| ©Травкин Е.И., Васильев Д.А. 2017. |  |
| © Курская академия государственной и  муниципальной службы, 2017. |  |

Курск 2017

1. **Структура программы повышения квалификации**

Общая характеристика дополнительной образовательной программы:

Законодательные и нормативные правовые акты, в соответствии с которыми разработана программа:

Федеральный закон от 09.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;

Приказ Минобрнауки России от 01.07.2013 № 499 «Об утверждении порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам» (зарегистрирован в Минюсте России 20.08.2013 № 29444);

Квалификационный справочник должностей руководителей, специалистов и других служащих, утвержденный Постановлением Минтруда России от 21.08.1998 № 37 (в ред. приказов Минздравсоцразвития России от 25.07.2005 № 461, от 07.11.2006 № 749, от 17.09.2007 № 605, от 29.04.2008 № 200, от 14.03.2011 № 194, от 15.05.2013 № 205).

Федеральный закон от 27.10.2004 №79-ФЗ «О государственной гражданской службе Российской Федерации»

Федеральный закон от 9.02.2009 г. №8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»

Закон Курской области от 18.06.2014 №42-ЗКО «О государственной гражданской службе Курской области»

Тип дополнительной профессиональной программы: программа повышения квалификации (далее - программа).

Программа разработана с учетом квалификационных требований к результатам освоения образовательных программ и направлена на качественное изменение профессиональных компетенций в рамках имеющийся квалификации, необходимой для профессиональной деятельности, и (или) повышение профессионального уровня в рамках имеющейся квалификации.

К освоению программы допускаются: лица, имеющие высшее или среднее профессиональное образование, а также лица, получающие высшее или среднее профессиональное образование.

Обучение по программе осуществляется на основе договора об образовании, заключаемого со слушателем и (или) с физическим или юридическим лицом, обязующимся оплатить обучение лица, зачисляемого на обучение, либо за счет бюджетных ассигнований федерального бюджета, бюджетов субъектов РФ.

Срок освоения программы: 23 часа (0,64 зачетные единицы). Срок освоения может определяться договором об образовании.

Форма обучения: очная, с отрывом от работы.

Категория обучающихся:

* руководители и специалисты департаментов, комитетов, управлений.

Формы аттестации: промежуточная аттестация - после освоения соответствующего раздела учебного плана программы, итоговая аттестация - после освоения всех модулей программы.

Выдаваемый документ: лицам, успешно освоившим программу и прошедшим итоговую аттестацию, выдается удостоверение о повышении квалификации.

При освоении программы параллельно с получением высшего или среднего профессионального образования удостоверение о повышении квалификации выдается одновременно с получением соответствующего документа об образовании.

Программа является преемственной к основной образовательной программе высшего образования направления подготовки 10.03.01 Информационная безопасность (уровень бакалавриата)

1. **Цели обучения**

В результате освоения программы предусмотрено совершенствование компетенций необходимых для профессиональной деятельности слушателей, и повышения их профессионального уровня в рамках имеющейся квалификации:

Перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения:

* способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты.
* способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;
* способностью администрировать подсистемы информационной безопасности объекта защиты;
* способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты;
* способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации;
* способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации;
* способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений;
* способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов;
* способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности;
* способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности;
* способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации;
* способность понимать сущность и значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска и обработки больших объемов информации по профилю деятельности в глобальных компьютерных системах, сетях, в библиотечных фондах и в иных источниках информации;
* способностью учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности;
* способностью работать с программными средствами прикладного, системного и специального назначения;
* способностью применять современные методы и средства исследований для обеспечения информационной безопасности компьютерных систем;
* способностью проводить анализ безопасности ИСПДН с использованием отечественных и зарубежных стандартов в области компьютерной безопасности;
* способностью проводить обоснование и выбор рационального решения по уровню защищенности ИСПДН с учетом заданных требований;
* способностью проводить сбор и анализ исходных данных для проектирования систем защиты информации в ИСПДН;
* способностью проводить анализ проектных решений по обеспечению защищенности ИСПДН;
* способностью участвовать в разработке системы защиты информации предприятия (организации) и подсистемы информационной безопасности ИСПДН;
* способностью к проведению экспериментального исследования компьютерных систем с целью выявления уязвимостей;
* способностью оценивать эффективность систем защиты информации в ИСПДН;
* способностью производить установку, тестирование программного обеспечения и программно-аппаратных средств по обеспечению информационной безопасности ИСДН;
* способностью принимать участие в эксплуатации программного обеспечения и программно-аппаратных средств обеспечения информационной безопасности ИСПДН;
* способностью выполнять работы по приему, настройке, регулировке, освоению и восстановлению работоспособности оборудования защиты информации;
* способностью разрабатывать и составлять инструкции и руководства пользователей по эксплуатации средств обеспечения информационной безопасности компьютерных систем и аппаратно-программных средств защиты информации .

Развитие умений и навыков, необходимых для выполнения соответствующих функций:

* установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований;
* участие в проведении аттестации объектов информатизации по требованиям безопасности;
* администрирование подсистем информационной безопасности объекта;
* информации и аудите информационной безопасности автоматизированных систем;
* сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности;
* проведение проектных расчетов элементов систем обеспечения информационной безопасности;
* участие в разработке технологической и эксплуатационной документации;
* проведение предварительного технико-экономического обоснования проектных расчетов;
* сбор, изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования;
* осуществление организационно-правового обеспечения информационной безопасности объекта защиты;
* изучение и обобщение опыта работы других учреждений, организаций и предприятий в области защиты информации, в том числе информации ограниченного доступа;
* контроль эффективности реализации политики информационной безопасности объекта защиты.

1. **Планируемые результаты обучения**

В результате освоения программы слушатель должен приобрести следующие знания и умения, необходимые для качественного изменения компетенций, указанных в разделе 2:

Слушатель должен знать:

* принципы организации и этапы разработки комплексной системы защиты информации;
* факторы, влияющие на организацию комплексной системы защиты информации;
* методики анализа и оценки угроз безопасности информации;
* методы определения потенциальных каналов несанкционированного доступа к информации;
* условия функционирования комплексной системы защиты информации;
* о технологическом и организационном построении комплексной системы защиты информации;
* о кадровом обеспечении функционирования комплексной системы защиты информации;
* назначение, структуру и содержание управления комплексной системы защиты информации;
* принципы и методы планирования функционирования комплексной системы защиты информации;
* сущность и содержание контроля функционирования комплексной системы защиты информации;
* состав методов и моделей оценки эффективности комплексной системы защиты информации;
* основные особенности современного состояния организационно-правового обеспечения защиты персональных данных в информационных системах персональных данных;
* проблемы охраны конфиденциальности персональных данных лиц в Российской Федерации;
* подходы к правовой защите персональных данных, организации контроля за возможными каналами их утечки;
* методы и способы выявления угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
* порядок организации работ по обеспечению безопасности информации в информационных системах персональных данных;
* требования и рекомендации по обеспечению безопасности информации в информационных системах персональных данных;
* знать основные технические, программные, криптографические, программно-аппаратные средства, применяемые для защиты персональных данных;
* методы контроля и оценки состояния обеспечения безопасности информации в информационных системах персональных данных;

Слушатель должен уметь:

* владеть навыками в области анализа предметной области и выявления направлений совершенствования функционирования системы защиты;
* иметь опыт определения и нормативного закрепления состава защищаемой информации;
* составлять перечень сведений, отнесенных к персональным данным и проводить их классификацию;
* проводить классификацию информационных систем персональных данных с составлением соответствующего акта;
* выявлять актуальные угрозы безопасности информации в информационных системах персональных данных;
* разрабатывать частные модели угроз безопасности персональных данных в конкретных информационных системах персональных данных с учетом их назначения, условий и особенностей функционирования;
* разрабатывать техническое обоснование для создания системы защиты информационных систем персональных данных;
* оформлять техническое (частное техническое) задание на разработку системы (подсистемы) защиты персональных данных;
* разрабатывать необходимую организационно-распорядительную и нормативно-техническую документацию в интересах организации защиты персональных данных;
* планировать, организовывать и контролировать выполнение работ и мероприятий по защите персональных данных;
* оценивать эффективность защиты информационных систем персональных данных.

Слушатель должен владеть навыками:

* выявления и оценки источников, способов и результатов дестабилизирующего воздействия на информацию;
* определения возможностей несанкционированного доступа к защищаемой информации;
* определением компонентов эффективности комплексной системы защиты информации;
* разработки модели эффективности комплексной системы защиты информации;
* применения технических, криптографических, программно-аппаратных и программных средств защиты персональных данных;
* разработки внутренних нормативных документов, обеспечивающих защиту персональных данных в информационных системах персональных данных.

1. **Учебный план**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № п/п | Наименование разделов | Всего часов | В том числе: | | Формы контроля |
| Лекции | Практические занятия |
| **Базовая часть** | | | | | |
|  | Учебный раздел Р.1.  Комплексная защита информации | 10 | 8 | 2 | Собеседование |
| **Профильная часть** | | | | | |
| 2 | Учебный раздел Р.2.  Обеспечение безопасности персональных данных | 13 | 10 | 3 | Собеседование |
|  | Итоговая аттестация |  |  |  | Экзамен в форме тестирования |
| Итого: | | 23 | 18 | 5 |  |

**Учебно-тематический план**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № п/п | Наименование разделов, дисциплин и тем | Всего часов | В том числе: | | | Формы контроля |
| Лекции | Выездные занятия, стажировка, деловые игры и др. | Практические занятия |
| **Базовая часть** | | | | | | |
| 1. | **Учебный раздел Р.1**  **Комплексная защита информации** | **10** | **8** |  | **2** | **Собеседование** |
| 1.1 | Сущность и задачи комплексной системы защиты информации | 2 | 2 |  |  |  |
| 1.2 | Выявление угроз информационной безопасности | 2 | 2 |  |  |  |
| 1.3 | Определение компонентов и структуры комплексной системы защиты информации | 2 |  |  | 2 |  |
| 1.4 | Принципы организации и этапы разработки комплексной системы защиты информации | 2 | 2 |  |  |  |
| 1.5 | Экономическая эффективность комплексной системы защиты информации | 2 | 2 |  |  |  |
| **Профильная часть** | | | | | | |
| 2. | **Учебный раздел Р.2.**  **Обеспечение безопасности персональных данных** | **13** | **10** |  | **3** | **Собеседование** |
| 2.1 | Нормативно-правовое обеспечение безопасности персональных данных | 2 | 2 |  |  |  |
| 2.2 | Организация и обеспечение режимов защиты персональных данных. | 2 | 2 |  |  |  |
| 2.3 | Программно-аппаратные средства защиты информации, применяемые при защите информационных системах персональных данных | 2 | 2 |  |  |  |
| 2.4 | Криптографические средства защиты информации, применяемые при защите информационных системах персональных данных | 4 | 2 |  | 2 |  |
| 2.5 | Порядок создания и эксплуатации информационных систем персональных данных | 3 | 2 |  | 1 |  |
| 3. | Итоговая аттестация |  |  |  |  | Экзамен в форме тестирования |
| **Итого:** | | **23** | **18** |  | **5** |  |

1. **Календарный учебный график**

Календарный график определятся в соответствии с Постановлением Администрация Курской области от 30 декабря 2013 г. N 1047-па «Об утверждении плана развития государственной гражданской службы Курской области на 2014 - 2018 годы»

|  |  |  |  |
| --- | --- | --- | --- |
| Форма обучения | Часов в день (аудиторных) | Дней в неделю (аудиторных) | Общая продолжительность программы |
| Очная | 6 | 4 | 1 неделя |

1. **Рабочие программы учебных разделов (предметов, модулей)**

*Рабочая программа раздела 1 «Комплексная защита информации».*

Цели модуля: получение обновление и систематизация по созданию и функционированию комплексной системы защиты информации.

Тематическое содержание раздела 1.

**Сущность и задачи комплексной системы защиты информации.**

Понятие и сущность комплексной системы защиты информации. Назначение комплексной системы защиты информации. Задачи комплексной системы защиты информации. Принципы организации комплексной системы защиты информации. Основные факторы, влияющие на организацию комплексной системы защиты информации: организационно-правовая форма и характер основной деятельности предприятия; состав, объем и степень конфиденциальности защищаемой информации; структура и территориальное расположение предприятия; режим функционирования предприятия; конструктивные особенности предприятия; степень автоматизации основных процедур обработки защищаемой информации.

**Выявление угроз информационной безопасности.**

Определение источников дестабилизирующего воздействия на информацию и видов их воздействия. Выявление способов воздействия на информацию. Определение причин, обстоятельств и условий дестабилизирующего воздействия на информацию. Оценка ущерба от потенциального дестабилизирующего воздействия на информацию.

Выявление каналов и определение возможных методов несанкционированного доступа к информации. Анализ потенциальных последствий реализации несанкционированного доступа.

Выявление нарушителей (незаконных пользователей) и состава интересующей их информации. Определение направлений и возможностей доступа нарушителей к защищаемой информации. Оценка степени уязвимости информации в результате действий нарушителей различных категорий.

**Определение компонентов и структуры комплексной системы защиты информации.**

Объекты защиты как основной фактор, определяющий состав компонентов комплексной системы защиты информации. Выявление состава носителей защищаемой информации. Хранилища носителей информации как объект защиты. Особенности помещений для работы с защищаемой информацией как объектов защиты. Состав технических средств обработки, передачи, транспортировки и защиты информации, являющихся объектами защиты. Состав средств обеспечения функционирования предприятия, подлежащих защите. Факторы, определяющие необходимость защиты периметра и здания предприятия. Специфика персонала предприятия как объекта защиты. Выбор компонентов и определение структуры комплексной системы защиты информации.

**Принципы организации и этапы разработки комплексной системы защиты информации.**

Общее содержание работ по организации комплексной системы защиты информации. Характеристика основных стадий создания комплексной системы защиты информации. Предпроектное обследование, технический проект, рабочий проект. Апробация и ввод в эксплуатацию. Понятие и цели управления комплексной системы защиты информации. Сущность процессов управления комплексной системы защиты информации. Принципы управления комплексной системы защиты информации. Основные стили управления. Структура и содержание общей технологии управления комплексной системы защиты информации.

**Экономическая эффективность комплексной системы защиты информации**

Виды ущерба от несанкционированного доступа (НСД) к информации. Основные методы определения затрат на информационную безопасность. Основные положения определения экономической эффективности защиты информации.

*Рабочая программа раздела 2 «Обеспечение безопасности персональных данных».*

Цели модуля: качественное изменение компетенций указанных в разделе 2. программы.

Тематическое содержание раздела 2.

**Нормативно-правовое обеспечение безопасности персональных данных**

*Требования Федерального закона от 27 июля 2006 г. №152 к обеспечению безопасности персональных данных*

Основные понятия. Персональные данные в Федеральном законе и Трудовом кодексе Российской Федерации. Содержание категории «персональные данные». Область применения закона. Ограничения.

Обработка персональных данных: сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (передача), обезличивание, блокирование, уничтожение.

Принципы обработки персональных данных. Условия обработки персональных данных. Согласие субъекта. Обработка биометрических данных. Обработка персональных данных третьим лицом в интересах оператора. Трансграничная передача персональных данных. Специальные категории персональных данных и особенности их обработки. Права субъектов персональных данных и их соблюдение при обработке. Обязанности оператора персональных данных в ходе сбора и обработки персональных данных, ответы на запросы субъектов. Уведомления об обработке персональных данных в уполномоченный орган по защите прав субъектов персональных данных.

Контроль и надзор за обработкой персональных данных. Ответственность за нарушение требований по обращению с персональными данными.

*Требования Постановления Правительства Российской Федерации от 17 ноября 2007 г. № 781 к обеспечению безопасности персональных данных*

Требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

*Требования Приказа ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. N 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных»*

Требования. Порядок проведения классификации информационных систем персональных данных.

*Ведомственные нормативные документы по обеспечению защиты персональных данных в Российской Федерации*

Руководящие документы ФСТЭК и ФСБ России по защите персональных данных. Нормативно-методическое обеспечение безопасности информационных систем персональных данных в органах власти, учреждениях (предприятиях).

Порядок лицензирования операторов информационных систем персональных данных.

**Организация и обеспечение режимов защиты персональных данных**

Мероприятия по защите сведений конфиденциального характера, основные внутренние нормативные документы, меры по охране конфиденциальности; формирование перечня персональных данных.

Ограничение доступа к персональным данным, учет лиц, допущенных к персональным данным, определение порядка обращения с такими сведениями, контроля за его соблюдением, организация доступа к персональным данным, внутренние нормативные документы по охране конфиденциальности сведений, их содержание, порядок разработки и ввода в действие, контроль за соблюдением режима конфиденциальности;

Подготовка уведомлений об обработке персональных данных в уполномоченный орган.

**Организационные и организационно-технические мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных**

Понятие информационной системы персональных данных. Классификация информационных систем персональных данных. Порядок составления соответствующего акта.

Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Разработка частных моделей угроз безопасности персональных данных в конкретных информационных системах персональных данных с учетом их назначения, условий и особенностей функционирования.

Мероприятия по техническому обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных различных классов.

Мероприятия по оценке соответствия принятых мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных требованиям безопасности информации.

Требования к подготовке к утилизации и порядок утилизации персональных данных и машиночитаемых носителей информации, используемых в обработке персональных данных.

Защищенный электронный документооборот персональных данных. Использование электронной цифровой подписи в информационных системах персональных данных.

**Программно-аппаратные средства защиты информации, применяемые при защите информационных системах персональных данных**

Современные программно-аппаратные средства. Возможности и основы применения средств защиты информации от несанкционированного доступа, средств антивирусной защиты, средств сетевой защиты.

**Криптографические средства защиты информации, применяемые при защите информационных системах персональных данных**

Современные криптографические средства защиты информации. Возможности и применение шифровальных средств и средств ЭЦП.

**Порядок создания и эксплуатации информационных систем персональных данных**

Организация обеспечения безопасности персональных данных в информационных системах персональных данных. Техническое обоснование для создания системы защиты информационных систем персональных данных.

Оформление технического (частного технического) задания на разработку системы (подсистемы) защиты персональных данных.

Внедрение средств обеспечения информационной безопасности в информационных системах персональных данных.

Аттестация информационных систем персональных данных.

Техническое обслуживание и ремонт аттестованных информационных систем персональных данных.

Контроль обеспечения безопасности персональных данных.

Промежуточный контроль полученных знаний осуществляется по результатам обсуждения проблемных тем на собеседовании и в форуме для консультаций.

1. **Организационно-педагогические условия**

Форма организации образовательной деятельности.

Формат программы основан на модульном принципе представления содержания образовательной программы и построения учебных планов и содержит 2 учебных раздела, которые включают в себя перечень, трудоемкость, последовательность и распределение учебных разделов, иных видов учебной деятельности обучающихся и форм аттестации.

Образовательная деятельность обучающихся предусматривает следующие виды учебных занятий и учебных работ: лекции; практические занятия.

Условия реализация программы:

Обучение по программе осуществляется на основе договора об образовании, заключаемого со слушателем и (или) с физическим или юридическим лицом, обязующимся оплатить обучение лица, зачисляемого на обучение.

Обучение осуществляется единовременно и непрерывно, посредством освоения отдельных учебных разделов программы.

Требования к кадровому обеспечению учебного процесса: программа реализуется преподавателями Академии госслужбы.

Требования к учебно-методическому обеспечению учебного процесса: методическое обеспечение учебного процесса включает разработки кафедры: мультимедийные презентации, методические рекомендации и др.

Требования к материально-техническому обеспечению учебного процесса: процесс реализации Программы обеспечен необходимой материально-технической базой для проведения всех видов учебных занятий, предусмотренных учебным планом: лекционной, практической работы. Для эффективного проведения занятий предусмотрено использование современных технических средств обучения (мультимедийный проектор). Материально-техническое обеспечение соответствует действующей санитарно-технической норме.

*Литература:*

*нормативные правовые акты:*

1. Конституция Российской Федерации (с учетом поправок, внесенных Законами Российской Федерации о поправках к Конституции Российской Федерации от 30.12.2008 N 6-ФКЗ и от 30.12.2008 N 7-ФКЗ). Глава 2. Права и свободы человека и гражданина (ст.ст. 23-24).
2. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ (в ред. Федеральных законов от 25.04.2002 N 41-ФЗ, от 25.07.2002 N 112-ФЗ, от 30.10.2002 N 130-ФЗ, от 31.10.2002 N 133-ФЗ, от 31.12.2002 N 187-ФЗ, от 30.06.2003 N 86-ФЗ, от 04.07.2003 N 94-ФЗ, от 04.07.2003 N 103-ФЗ, от 11.11.2003 N 138-ФЗ, от 11.11.2003 N 144-ФЗ, от 08.12.2003 N 161-ФЗ, от 08.12.2003 N 169-ФЗ, от 23.12.2003 N 185-ФЗ, от 09.05.2004 N 37-ФЗ, от 26.07.2004 N 77-ФЗ, от 28.07.2004 N 93-ФЗ, от 20.08.2004 N 114-ФЗ, от 20.08.2004 N 118-ФЗ, от 25.10.2004 N 126-ФЗ, от 28.12.2004 N 183-ФЗ, от 28.12.2004 N 187-ФЗ, от 30.12.2004 N 211-ФЗ, от 30.12.2004 N 214-ФЗ, от 30.12.2004 N 219-ФЗ (ред. 21.03.2005), от 07.03.2005 N 14-ФЗ, от 07.03.2005 N 15-ФЗ, от 21.03.2005 N 19-ФЗ, от 21.03.2005 N 21-ФЗ, от 22.04.2005 N 38-ФЗ, от 09.05.2005 N 45-ФЗ, от 18.06.2005 N 66-ФЗ, от 02.07.2005 N 80-ФЗ, от 02.07.2005 N 82-ФЗ, от 21.07.2005 N 93-ФЗ, от 21.07.2005 N 113-ФЗ, от 22.07.2005 N 120-ФЗ, от 27.09.2005 N 124-ФЗ, от 05.12.2005 N 156-ФЗ, от 19.12.2005 N 161-ФЗ, от 26.12.2005 N 183-ФЗ, от 27.12.2005 N 193-ФЗ, от 31.12.2005 N 199-ФЗ, от 05.01.2006 N 7-ФЗ, от 05.01.2006 N 10-ФЗ, от 02.02.2006 N 19-ФЗ, от 03.03.2006 N 30-ФЗ, от 16.03.2006 N 41-ФЗ, от 15.04.2006 N 47-ФЗ, от 29.04.2006 N 57-ФЗ, от 08.05.2006 N 65-ФЗ, от 03.06.2006 N 73-ФЗ, от 03.06.2006 N 78-ФЗ, от 03.07.2006 N 97-ФЗ, от 18.07.2006 N 111-ФЗ, от 18.07.2006 N 121-ФЗ, от 26.07.2006 N 133-ФЗ, от 26.07.2006 N 134-ФЗ, от 27.07.2006 N 139-ФЗ, от 27.07.2006 N 153-ФЗ, от 16.10.2006 N 160-ФЗ, от 03.11.2006 N 181-ФЗ, от 03.11.2006 N 182-ФЗ, от 05.11.2006 N 189-ФЗ, от 04.12.2006 N 201-ФЗ, от 04.12.2006 N 203-ФЗ, от 18.12.2006 N 232-ФЗ, от 29.12.2006 N 258-ФЗ, от 29.12.2006 N 262-ФЗ, от 30.12.2006 N 266-ФЗ, от 30.12.2006 N 270-ФЗ, от 09.02.2007 N 19-ФЗ, от 29.03.2007 N 39-ФЗ, от 09.04.2007 N 44-ФЗ, от 09.04.2007 N 45-ФЗ, от 20.04.2007 N 54-ФЗ, от 07.05.2007 N 66-ФЗ, от 10.05.2007 N 70-ФЗ, от 22.06.2007 N 116-ФЗ, от 19.07.2007 N 141-ФЗ, от 24.07.2007 N 204-ФЗ, от 24.07.2007 N 210-ФЗ, от 24.07.2007 N 211-ФЗ, от 24.07.2007 N 218-ФЗ, от 02.10.2007 N 225-ФЗ, от 18.10.2007 N 230-ФЗ, от 08.11.2007 N 257-ФЗ, от 27.11.2007 N 273-ФЗ, от 01.12.2007 N 304-ФЗ, от 06.12.2007 N 333-ФЗ, от 03.03.2008 N 21-ФЗ, от 29.04.2008 N 58-ФЗ, от 13.05.2008 N 66-ФЗ, от 16.05.2008 N 74-ФЗ, от 14.07.2008 N 118-ФЗ, от 22.07.2008 N 126-ФЗ, от 22.07.2008 N 145-ФЗ, от 22.07.2008 N 148-ФЗ, от 08.11.2008 N 197-ФЗ, от 03.12.2008 N 240-ФЗ, от 03.12.2008 N 247-ФЗ, от 03.12.2008 N 250-ФЗ, от 25.12.2008 N 280-ФЗ, от 25.12.2008 N 281-ФЗ, от 26.12.2008 N 293-ФЗ, от 30.12.2008 N 309-ФЗ, от 09.02.2009 N 9-ФЗ, от 07.05.2009 N 86-ФЗ, от 03.06.2009 N 112-ФЗ, от 28.06.2009 N 122-ФЗ, от 28.06.2009 N 124-ФЗ, от 29.06.2009 N 133-ФЗ, от 29.06.2009 N 134-ФЗ, с изм., внесенными Федеральными законами от 24.07.2007 N 212-ФЗ, от 22.12.2008 N 272-ФЗ, от 09.02.2009 N 3-ФЗ, от 03.06.2009 N 104-ФЗ, от 03.06.2009 N 121-ФЗ). Статья 13.11. Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) Глава 13. Административные правонарушения в области связи и информации (ст.ст. 13.1 — 13.24). Раздел П. Особенная часть.
3. Трудовой кодекс Российской Федерации от 30 декабря 2001 г. № 197-ФЗ (в ред. Федеральных законов от 24.07.2002 N 97-ФЗ, от 25.07.2002 N 116-ФЗ, от 30.06.2003 N 86-ФЗ, от 27.04.2004 N 32-ФЗ, от 22.08.2004 N 122-ФЗ, от 29.12.2004 N 201-ФЗ, от 09.05.2005 N 45-ФЗ, от 30.06.2006 N 90-ФЗ, от 18.12.2006 N 232-ФЗ, от 30.12.2006 N 271-ФЗ, от 20.04.2007 N 54-ФЗ, от 21.07.2007 N 194-ФЗ, от 01.10.2007 N 224-ФЗ, от 18.10.2007 N 230-ФЗ, от 01.12.2007 N 309-ФЗ, от 28.02.2008 N 13-ФЗ, от 22.07.2008 N 157-ФЗ, от 23.07.2008 N 160-ФЗ, от 25.12.2008 N 280-ФЗ, от 25.12.2008 N 281-ФЗ, от 30.12.2008 N 309-ФЗ, от 30.12.2008 N 313-ФЗ, от 07.05.2009 N 80-ФЗ, с изм., внесенными Постановлением Конституционного Суда Российской Федерации от 15.03.2005 N 3-П, Определением Конституционного Суда Российской Федерации от 11.07.2006 N 213-О). Глава 14 «Защита персональных данных работника» (ст. ст. 85-90).
4. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (в ред. Федеральных законов от 27.05.1998 N 77-ФЗ, от 25.06.1998 N 92-ФЗ, от 09.02.1999 N 24-ФЗ, от 09.02.1999 N 26-ФЗ, от 15.03.1999 N 48-ФЗ, от 18.03.1999 N 50-ФЗ, от 09.07.1999 N 156-ФЗ, от 09.07.1999 N 157-ФЗ, от 09.07.1999 N 158-ФЗ, от 09.03.2001 N 25-ФЗ, от 20.03.2001 N 26-ФЗ, от 19.06.2001 N 83-ФЗ, от 19.06.2001 N 84-ФЗ, от 07.08.2001 N 121-ФЗ, от 17.11.2001 N 144-ФЗ, от 17.11.2001 N 145-ФЗ, от 29.12.2001 N 192-ФЗ, от 04.03.2002 N 23-ФЗ от 14.03.2002 N 29-ФЗ, от 07.05.2002 N 48-ФЗ, от 07.05.2002 N 50-ФЗ, от 25.06.2002 N 72-ФЗ, от 24.07.2002 N 103-ФЗ, от 25.07.2002 N 112-ФЗ, от 31.10.2002 N 133-ФЗ, от 11.03.2003 N 30-ФЗ, от 08.04.2003 N 45-ФЗ, от 04.07.2003 N 94-ФЗ, от 04.07.2003 N 98-ФЗ от 07.07.2003 N 111-ФЗ, от 08.12.2003 N 162-ФЗ, от 08.12.2003 N 169-ФЗ, от 21.07.2004 N 73-ФЗ, от 21.07.2004 N 74-ФЗ, от 26.07.2004 N 78-ФЗ, от 28.12.2004 N 175-ФЗ, от 28.12.2004 N 187-ФЗ, от 21.07.2005 N 93-ФЗ, от 19.12.2005 N 161-ФЗ, от 05.01.2006 N 11-ФЗ, от 27.07.2006 N 153-ФЗ, от 04.12.2006 N 201-ФЗ, от 30.12.2006 N 283-ФЗ, от 09.04.2007 N 42-ФЗ, от 09.04.2007 N 46-ФЗ, от 10.05.2007 N 70-ФЗ, от 24.07.2007 N 203-ФЗ, от 24.07.2007 N 211-ФЗ, от 24.07.2007 N 214-ФЗ, от 04.11.2007 N 252-ФЗ, от 01.12.2007 N 318-ФЗ, от 06.12.2007 N 333-ФЗ, от 06.12.2007 N 335-ФЗ, от 14.02.2008 N 11-ФЗ, от 08.04.2008 N 43-ФЗ, от 13.05.2008 N 66-ФЗ, от 22.07.2008 N 145-ФЗ, от 25.11.2008 N 218-ФЗ, от 25.12.2008 N 280-ФЗ, от 30.12.2008 N 321-ФЗ, от 13.02.2009 N 20-ФЗ, от 28.04.2009 N 66-ФЗ, от 03.06.2009 N 106-ФЗ, от 29.06.2009 N 141-ФЗ, с изм., внесенными Постановлением Конституционного Суда Российской Федерации от 27.05.2008 N 8-П, Федеральным законом от 22.12.2008 N 272-ФЗ). Статья 137. Нарушение неприкосновенности частной жизни. Глава 19. Преступления против конституционных прав и свобод человека и гражданина (ст.ст. 136-149). Раздел VII. Преступления против личности (ст.ст. 105-157). Особенная часть (ст.ст. 105-360) Статья 140. Отказ в предоставлении гражданину информации Глава 19. Преступления против конституционных прав и свобод человека и гражданина (ст.ст. 136-149). Раздел VII. Преступления против личности (ст.ст. 105-157). Особенная часть (ст.ст. 105-360). Статья 272. Неправомерный доступ к компьютерной информации Глава 28. Преступления в сфере компьютерной информации (ст.ст. 272-274). Раздел IX. Преступления против общественной безопасности и общественного порядка (ст.ст. 205-274). Особенная часть (ст.ст. 105-360).
5. Федеральный закон от 19 декабря 2005 г. N 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных».
6. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
7. Федеральный закон Российской Федерации от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи» (в ред. Федерального закона от 08.11.2007 N 258-ФЗ).
8. Федеральный закон от 22 октября 2004 г. № 125-ФЗ «Об архивном деле в Российской Федерации» (в ред. Федеральных законов от 04.12.2006 N 202-ФЗ, от 01.12.2007 N 318-ФЗ, от 13.05.2008 N 68-ФЗ). Глава 4. Хранение и учет архивных документов (ст.ст. 17— 19). Глава И. Государственные реестры (ст.ст. 4 -7).
9. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
10. Федеральный закон Российской Федерации 29 июля 2004 г. N 98-ФЗ «О коммерческой тайне» (в ред. Федеральных законов от 02.02.2006 N 19-ФЗ, от 18.12.2006 N 231-ФЗ, от 24.07.2007 N 214-ФЗ).
11. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Перечень сведений конфиденциального характера» (в ред. Указа Президента Российской Федерации от 23.09.2005 N 1111).
12. 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» (в ред. Указа Президента Российской Федерации от 21.10.2008 N 1510).
13. Основы законодательства Российской Федерации об охране здоровья граждан от 22 июля 1993 г. № 5487-1 (в ред. Федеральных законов от 02.03.1998 N 30-ФЗ, от 20.12.1999 N 214-ФЗ, от 02.12.2000 N 139-ФЗ, от 10.01.2003 N 15-ФЗ, от 27.02.2003 N 29-ФЗ, от 30.06.2003 N 86-ФЗ, от 29.06.2004 N 58-ФЗ, от 22.08.2004 N 122-ФЗ (ред. 29.12.2004), от 01.12.2004 N 151-ФЗ, от 07.03.2005 N 15-ФЗ, от 21.12.2005 N 170-ФЗ, от 31.12.2005 N 199-ФЗ, от 02.02.2006 N 23-ФЗ, от 29.12.2006 N 258-ФЗ (ред. 18.10.2007), от 24.07.2007 N 214-ФЗ, от 18.10.2007 N 230-ФЗ, от 23.07.2008 N 160-ФЗ, от 08.11.2008 N 203-ФЗ, от 25.12.2008 N 281-ФЗ, от 30.12.2008 N 309-ФЗ, с изм., внесенными Указом Президента Российской Федерации от 24.12.1993 N 2288). Статья 61. Врачебная тайна.
14. Постановление Правительства Российской Федерации от 16 марта 2009 г. N 228 «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций».
15. Постановление Правительства Российской Федерации от 6 июня 2007 г. № 353 «Вопросы Федеральной службы по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия» (в ред. Постановлений Правительства Российской Федерации от 15.12.2007 N 878, от 28.12.2007 N 938).
16. Постановление Правительства Российской Федерации от 27 сентября 2007 г. № 612 «Об утверждении Правил продажи товаров дистанционным способом». Пункт 16.
17. Постановление Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».
18. Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 г. «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
19. Постановление Правительства Российской Федерации от 15 августа 2006 г. №504 «О лицензировании деятельности по технической защите конфиденциальной информации».
20. Постановление Правительства Российской Федерации от 31.08.2006 «О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации».

*нормативно-методические и методические документы:*

1. Приказ Федеральной службы по техническому и экспортному контролю, ФСБ России и Министерства информационных технологий и связи Российской Федерации от 13 февраля 2008 г. №55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных».
2. Приказ Министерства связи и массовых коммуникаций Российской Федерации от 5 августа 2008 г. № 21 «Об утверждении Типового положения о территориальном органе Федеральной службы по надзору в сфере связи и массовых коммуникаций».
3. Приказ Федеральной службы по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия от 28 марта 2008 г. №154 «Об утверждении положения о ведении реестра операторов, осуществляющих обработку персональных данных».
4. Положение о Федеральной службе по техническому и экспортному контролю (утв. Указом Президента Российской Федерации от 16 августа 2004 г. № 1085) (в ред. Указов Президента Российской Федерации от 30.11.2006 N 1321, от 23.10.2008 N 1517, от 17.11.2008 N 1625).
5. Положение о Федеральной службе безопасности Российской Федерации (утв. Указом Президента Российской Федерации от 11 августа 2003 г. N 960) (в ред. Указов Президента Российской Федерации от 11.07.2004 N 870, от 31.08.2005 N 1007, от 12.06.2006 N 602, от 27.07.2006 N 799, от 28.12.2006 N 1476, от 28.11.2007 N 1594, от 28.12.2007 N 1765, от 01.09.2008 N 1278, от 23.10.2008 N 1517, от 17.11.2008 N 1625).
6. Руководящий документ. Типовое положение об органе по аттестации объектов информатизации по требованиям безопасности информации. Утверждено Председателем Государственной технической комиссии при Президенте Российской Федерации 25.11.1994.
7. Руководящий документ. Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных. Утверждены Заместителем директора ФСТЭК России от 15.02.2008.
8. Руководящий документ. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены Заместителем директора ФСТЭК России от 15.02.2008.
9. Руководящий документ. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены Заместителем директора ФСТЭК России от 15.02.2008.
10. Руководящий документ. Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены Заместителем директора ФСТЭК России от 15.02.2008.
11. Руководящий документ. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации. Утверждены руководством 8 Центра ФСБ России 21.02.2008 № 149/5-144.
12. Руководящий документ. Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены руководством 8 Центра ФСБ России 21.02.2008 № 149/6/6-622.
13. Руководящий документ. «Методические рекомендации по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах» разработаные Управлением ФСТЭК России по УрФО, 2009 г.

*стандарты:*

1. ГОСТ ИСО/МЭК 15408-1-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.
2. ГОСТ Р ИСО/МЭК 15408-2-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности.
3. ГОСТ Р ИСО/МЭК 15408-3-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности.
4. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью.
5. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.
6. ГОСТ Р 50739-95. СВТ. Защита от несанкционированного доступа к информации.
7. ГОСТ Р 50752-95. Информационная технология. Защита информации от утечки за счет побочных электромагнитных излучений при ее обработке средствами вычислительной техники. Методы испытаний.
8. ГОСТ Р 50922-2006. Защита информации. Основные термины определения.
9. ГОСТ Р 51624-2000. Автоматизированные системы в защищенном исполнении. Общие требования.
10. ГОСТ Р 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.
11. ГОСТ Р 51583-2000. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения.
12. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от НСД к информации. Общие технические требования.
13. ГОСТ 34.602-89. Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы.

*учебная и учебно-методическая литература:*

1. Воробьев Е.Г. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]: учебное пособие/ Воробьев Е.Г.— Электрон. текстовые данные.— СПб.: Интермедия, 2017.— 432 c.— Режим доступа: http://www.iprbookshop.ru/66796.html.— ЭБС «IPRbooks»
2. Демидов А.А. Проблемы контроля безопасности информации на объектах телекоммуникационных систем органов государственного управления [Электронный ресурс]: учебное пособие/ Демидов А.А.— Электрон. текстовые данные.— СПб.: Университет ИТМО, 2015.— 70 c.— Режим доступа: http://www.iprbookshop.ru/67555.html.— ЭБС «IPRbooks»
3. Исаев А.С. Правовые основы организации защиты персональных данных [Электронный ресурс]: учебное пособие/ Исаев А.С., Хлюпина Е.А.— Электрон. текстовые данные.— СПб.: Университет ИТМО, 2014.— 106 c.— Режим доступа: http://www.iprbookshop.ru/67564.html.— ЭБС «IPRbooks»
4. Катаржнов А.Д. Организационно-распорядительные документы органов власти, муниципальных образований и предприятий по защите персональных данных [Электронный ресурс]: учебное пособие/ Катаржнов А.Д.— Электрон. текстовые данные.— СПб.: Университет ИТМО, 2016.— 136 c.— Режим доступа: http://www.iprbookshop.ru/67450.html.— ЭБС «IPRbooks»
5. Комплексное обеспечение информационной безопасности автоматизированных систем [Электронный ресурс]: лабораторный практикум/ М.А. Лапина [и др.].— Электрон. текстовые данные.— Ставрополь: Северо-Кавказский федеральный университет, 2016.— 242 c.— Режим доступа: http://www.iprbookshop.ru/62945.html.— ЭБС «IPRbooks»
6. Петренко В.И. Защита персональных данных в информационных системах [Электронный ресурс]: учебное пособие/ Петренко В.И.— Электрон. текстовые данные.— Ставрополь: Северо-Кавказский федеральный университет, 2016.— 201 c.— Режим доступа: http://www.iprbookshop.ru/66023.html.— ЭБС «IPRbooks»
7. Рагозин Ю.Н. Инженерно-техническая защита информации [Электронный ресурс]: учебное пособие по физическим основам образования технических каналов утечки информации и по практикуму оценки их опасности/ Рагозин Ю.Н.— Электрон. текстовые данные.— СПб.: Интермедия, 2018.— 168 c.— Режим доступа: http://www.iprbookshop.ru/73641.html.— ЭБС «IPRbooks»
8. Скрипник Д.А. Обеспечение безопасности персональных данных [Электронный ресурс]/ Скрипник Д.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 121 c.— Режим доступа: http://www.iprbookshop.ru/52153.html.— ЭБС «IPRbooks»
9. Цуканова О.А. Экономика защиты информации [Электронный ресурс]: учебное пособие/ Цуканова О.А., Смирнов С.Б.— Электрон. текстовые данные.— СПб.: Университет ИТМО, 2014.— 90 c.— Режим доступа: http://www.iprbookshop.ru/65371.html.— ЭБС «IPRbooks»
10. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс]/ Шаньгин В.Ф.— Электрон. текстовые данные.— Саратов: Профобразование, 2017.— 702 c.— Режим доступа: http://www.iprbookshop.ru/63594.html.— ЭБС «IPRbooks»
11. **Оценочные материалы**

**Вопросы для подготовки к итоговой аттестации**

1. Методологические основы организации комплексной системы защиты информации
2. Система управления информационной безопасностью предприятия. Принципы построения и взаимодействие с другими подразделениями
3. Требования к организационной и технической составляющим комплексной системы защиты информации
4. Требования по безопасности, предъявляемые к изделиям информационных технологий (ИТ)
5. Этапы разработки комплексной системы защиты информации
6. Классификация информации по видам тайны и степеням конфиденциальности
7. Нормативно-правовые аспекты определения состава защищаемой информации
8. Методика определения состава защищаемой информации
9. Порядок внедрения Перечня сведений, составляющих коммерческой тайны, внесение в него изменений и дополнений
10. Методика выявления состава носителей защищаемой информации
11. Особенности взаимоотношений с контрагентами как объект защиты информации ограниченного доступа
12. Факторы, определяющие необходимость защиты периметра и здания предприятия
13. Особенности помещений как объектов защиты для работы по защите информации
14. Факторы, создающие угрозу информационной безопасности
15. Угрозы безопасности информации
16. Модели нарушителей безопасности автоматизированных систем (АС)
17. Подходы к оценке ущерба от нарушений информационной безопасности (ИБ)
18. Технические каналы утечки информации, их классификация
19. Оптимальное построение системы защиты для АС
20. Проектирование системы защиты информации для существующей АС
21. Содержание концепции построения комплексной системы защиты информации
22. Разработка модели комплексной системы защиты информации
23. Технологическое и организационное построение комплексной системы защиты информации
24. Кадровое обеспечение функционирования комплексной системы защиты информации
25. Материально-техническое и нормативно-методическое обеспечение комплексной системы защиты информации
26. Назначение, структура и содержание управления комплексной системы защиты информации
27. Принципы и методы планирования функционирования комплексной системы защиты информации
28. Сущность и содержание контроля функционирования комплексной системы защиты информации
29. Управление комплексной системой защиты информации в условиях чрезвычайных ситуаций
30. Общая характеристика подходов к оценке эффективности комплексной системой защиты информации
31. Экономический подход к оценке эффективности комплексной системой защиты информации
32. Обработка персональных данных: сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (передача), обезличивание, блокирование, уничтожение.
33. Принципы обработки персональных данных.
34. Условия обработки персональных данных.
35. Согласие субъекта. Обработка биометрических данных.
36. Обработка персональных данных третьим лицом в интересах оператора.
37. Трансграничная передача персональных данных.
38. Специальные категории персональных данных и особенности их обработки.
39. Права субъектов персональных данных и их соблюдение при обработке.
40. Обязанности оператора персональных данных в ходе сбора и обработки персональных данных, ответы на запросы субъектов.
41. Уведомления об обработке персональных данных в уполномоченный орган по защите прав субъектов персональных данных.
42. Контроль и надзор за обработкой персональных данных. Ответственность за нарушение требований по обращению с персональными данными.
43. Требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.
44. Порядок проведения классификации информационных систем персональных данных.
45. Руководящие документы ФСТЭК и ФСБ России по защите персональных данных. Нормативно-методическое обеспечение безопасности информационных систем персональных данных в органах власти, учреждениях (предприятиях).
46. Порядок лицензирования операторов информационных систем персональных данных.
47. Мероприятия по защите сведений конфиденциального характера, основные внутренние нормативные документы, меры по охране конфиденциальности; формирование перечня персональных данных.
48. Ограничение доступа к персональным данным, учет лиц, допущенных к персональным данным, определение порядка обращения с такими сведениями, контроля за его соблюдением, организация доступа к персональным данным, внутренние нормативные документы по охране конфиденциальности сведений, их содержание, порядок разработки и ввода в действие, контроль за соблюдением режима конфиденциальности;
49. Подготовка уведомлений об обработке персональных данных в уполномоченный орган.
50. Понятие информационной системы персональных данных.
51. Классификация информационных систем персональных данных.
52. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных.
53. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.
54. Разработка частных моделей угроз безопасности персональных данных в конкретных информационных системах персональных данных с учетом их назначения, условий и особенностей функционирования.
55. Мероприятия по техническому обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных различных классов.
56. Мероприятия по оценке соответствия принятых мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных требованиям безопасности информации.
57. Требования к подготовке к утилизации и порядок утилизации персональных данных и машиночитаемых носителей информации, используемых в обработке персональных данных.
58. Защищенный электронный документооборот персональных данных. Использование электронной цифровой подписи в информационных системах персональных данных.
59. Современные программно-аппаратные средства. Возможности и основы применения средств защиты информации от несанкционированного доступа, средств антивирусной защиты, средств сетевой защиты.
60. Криптографические средства защиты информации, применяемые при защите информационных системах персональных данных
61. Организация обеспечения безопасности персональных данных в информационных системах персональных данных. Техническое обоснование для создания системы защиты информационных систем персональных данных.
62. Оформление технического (частного технического) задания на разработку системы (подсистемы) защиты персональных данных.
63. Внедрение средств обеспечения информационной безопасности в информационных системах персональных данных.
64. Аттестация информационных систем персональных данных.
65. Техническое обслуживание и ремонт аттестованных информационных систем персональных данных.
66. Контроль обеспечения безопасности персональных данных.

**Примерные тесты для проведения итоговой аттестации**

**Учебный раздел Р.1 Комплексная защита информации**

1. Совершенный этап защиты информации называется:

1.1. информационным

1.2. начальным

1.3. развитым\*

1.4. комплексным.

2. Процесс защиты информации в АС измеряется периодом:

2.1. 20 – 25 лет

2.2. 30 – 35 лет

2.3. 35 – 40 лет\*

2.4. 40 – 45 лет

3. Используемые средства защиты информации в АСОД на начальном этапе:

3.1. материальные

3.2. морально-этические

3.3. неформальные

3.4. формальные\*

4. Если информация искажена умышленно, то ее называют:

4.1. некачественной

4.2. субъективной

4.3. неполной

4.4. дезинформацией\*

5. Защита информации в АСОД считается комплексной, если:

5.1. реализуется одна цель защиты и используется один вид защиты

5.2. реализуется более одной цели защиты и используется более одного вида защиты

5.3. реализуются все цели защиты и используются все виды защиты\*

5.4. реализуется более одной цели защиты, но не все и используется более одного вида защиты, но не все

6. Если доступ к информации ограничивается, то такая информация является:

6.1. качественной

6.2. достоверной

6.3. конфиденциальной\*

6.4. ценной

7. Основной объем информации, составляющий базис организации или учреждения:

7.1. постоянная информация

7.2. медленно меняющаяся информация\*

7.3. техническая информация

7.4. быстро меняющаяся информация

8. При информационном обеспечении деятельности предприятия с точки зрения защиты информации предметом наиболее пристального внимания должна быть:

8.1. регулирование входных и выходных потоков информации

8.2. управление входными потоками информации

8.3. формирование и совершенствование информационного кадастра

8.4. информационный кадастр и информационные технологии\*

9. Традиционные меры защиты информации твердых копий:

9.1. программные средства

9.2. криптографические

9.3. соблюдение режима секретности\*

9.4. каровое обеспечение

10. Если носители информации являются электромагнитные волны, то такая информация относится к:

10.1. электронной

10.2. телекоммуникационной\*

10.3. документальной

10.4. речевой

11. Специализация функций АС, где особое значение имеет защита авторского права:

11.1. планирование и управление

11.2. образование и культура

11.3. транспорт и связь

11.4. научая и проектная деятельность\*

12. К какой из составляющих системы защиты информации относятся средства пожарной сигнализации и пожаротушения:

12.1. организационной

12.2. программной

12.3. технической\*

12.4. информационно-лингвистической

13. К какому виду угроз для АС относятся радиоактивное излучение и осадки:

13.1. природные\*

13.2. технические

13.3. созданные людьми преднамеренно

13.4. созданные людьми непреднамеренно

14. При выполнении курсовой или дипломной работы студент может быть допущен к сведениям, имеющим гриф секретности:

14.1. секретно\*

14.2. совершенно секретно

14.3. особой важности

14.4. для служебного пользования

15. Орган управления государственной системой защиты информации:

15.1. федеральное агентство правительственной связи и информации

15.2. федеральная служба контрразведки

15.3. гостехкомиссия России\*

15.4. федеральная служба безопасности

16. Какой из способов подключения к Интернету обеспечивает наибольшие возможности для доступа к информационным ресурсам:

16.1. по телефонному каналу, который коммутируется

16.2. постоянное соединение по оптоволоконному каналу\*

16.3. постоянное соединение по выделенному телефонному каналу

16.4. терминальное соединение по телефонному каналу, который коммутируется

17. Требование о возмещении убытков в связи с разглашением информации ограниченного доступа не может быть удовлетворено в случае:

17.1. несоблюдения пропускного режима

17.2. непринятие мер по соблюдению конфиденциальности\*

17.3. отсутствия пожарной сигнализации

17.4. отсутствия инженерных сооружений

18. Разрешать и ограничивать доступ к информации, определять порядок и условия доступа вправе:

18.1 президент РФ

18.2 гостехкомиссия России

18.3 оператор информационной системы

18.4 обладатель информации\*

19. Основанием для отказа гражданину в допуске к государственной тайне могут являться:

19.1. уклонение от воинской службы

19.2. принадлежность к общественным объединениям

19.3. имущественное и должностное понижение

19.4. уклонение от проверочных мероприятий\*

20. Степени секретности сведений и их грифы, составляющих государственную тайну:

20.1. особо секретно, совершенно секретно, секретно

20.2. очень секретно, неприкосновенно, секретно

20.3. совершенно секретно, тайно, секретно

20.4. особой важности, совершенно секретно, секретно\*

21. Какую функцию выполняет периферийное устройство:

21.1. управления работой ЭВМ по заданной программе

21.2. оперативного сохранения информации

21.3. ввода и вывода информации\*

21.4. никаких функций не выполняет

22. Средства защиты информации без участия человека называются:

22.1. законодательные

22.2. организационные

22.3. неформальные

22.4. формальные\*

23. К какому виду относится информация, если она представлена на диске:

23.1. телекоммуникационная

23.2. документальная\*

23.3. электронная

23.4. магнитная

24. К какой из составляющих системы защиты информации относится охрана территории и помещений:

24.1. кадровое обеспечение

24.2. организационные\*

24.3. программные

24.4. технические

25. Заражение компьютерными вирусами может осуществляться в процессе:

25.1. печати на принтере

25.2. работы с файлами\*

25.3. форматирования дискеты

25.4. выключения компьютера

26. Основу средств защиты информации составляют средства:

26.1. формальные

26.2. неформальные\*

26.3. программные

26.4. технические

27. Достоверность информации — это:

27.1. соответствие действительной обстановке\*

27.2. соответствие искомого и найденного

27.3. достаточность данных

27.4. соответствие текущему моменту

28. Способ защиты информации, при котором конкурент вводится в заблуждение относительно деятельности и намерений:

28.1. кодирование

28.2. криптография

28.3. управление

28.4. маскировка\*

29. Какое устройство может влиять на здоровье человека:

29.1. принтер

29.2. монитор\*

29.3. системный блок

29.4. модем

30. Производительность работы компьютера (скорость выполнения операций) зависит от:

30.1. размера экран

30.2. напряжения питания

30.3. скорости нажатия на клавиши

30.4. частоты процессора\*

**Учебный раздел Р.2. Обеспечение безопасности персональных данных**

1. Угрозы безопасности ПДн:

*а)* *совокупность* *условий* *факторов,* *создающих* *опасность* *несанкционированного,* *в* *том* *числе* *случайного,* *доступа* *к* *ПДн,* *результатом* *которого* *может* *стать* *уничтожение,* *изменение,* *блокирование,* *копирование,* *распространение* *ПДн,* *а* *также* *иных* *несанкционированных* *действий* *при* *их* *обработке* *в* *ИСПДн;*

б) совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности персональных данных;

в) только стихийное или бедствие техногенного характера.

2. Несанкционированный доступ (НСД) к информации:

*а)* *доступ* *к* *информации,* *нарушающий* *установленные* *правила* *разграничения* *доступа,* *с* *использованием* *штатных* *средств,* *предоставляемых* *средствами* *вычислительной* *техники* *(СВТ)* *или* *автоматизированными* *системами* *(АС);*

б) доступ к информации, нарушающий установленные правила разграничения доступа, с использованием специально разработанных технических средств;

в) копирование, искажение или модификация информации с нарушением установленных правил разграничения доступа.

3. Какие из перечисленных угроз относятся к случайным угрозам компьютерной информации:

а) несанкционированный доступ к информации, вредительские программы;

б) электромагнитные излучения и наводки, несанкционированная модификация структур;

*в)* *стихийные* *бедствия* *и* *аварии,* *сбои* *и* *отказы* *технических* *средств,* *ошибки* *пользователей* *и* *обслуживающего* *персонала.*

4. Для защиты от случайных угроз компьютерной информации используют:

а) обучение пользователей правилам работы с КС, разрешительную систему доступа в помещение;

б) межсетевые экраны, идентификацию и аутентификацию пользователей;

*в)* *дублирование* *информации,* *создание* *отказоустойчивых* *КС,* *блокировка* *ошибочных* *операций.*

5. Системы анализа уязвимостей позволяют:

а) выявить злоумышленника работающего в компьютерной сети;

б) выявить уязвимости проектируемой системы защиты информации; *в)* *выявить* *уязвимости* *действующей* *системы* *защиты* *информации.*

6. Персональные данные:

*а)* *информация,* *относящаяся* *к* *прямо* *или* *косвенно* *определенному* *или* *определяемому* *физическому* *лицу;*

б) данные, касающиеся состояния здоровья и религиозных взглядов человека; в) информация о месте работы, паспортные данные, сведения о доходе.

7. Обработка персональных данных:

*а)* *действие* *(операция)* *или* *совокупность* *действий* *(операций),* *совершаемых* *с* *использованием* *средств* *автоматизации* *или* *без* *использования* *таких* *средств* *с* *персональными* *данными,* *включая* *сбор,* *запись,* *систематизацию,* *накопление,* *хранение,* *уточнение* *(обновление,* *изменение),* *извлечение,* *использование,* *передачу* *(распространение,* *предоставление,* *доступ),* *обезличивание,* *блокирование,* *удаление,* *уничтожение* *персональных* *данных;*

б) накопление, хранение и передача персональных данных;

в) размещение персональных данных в информационных системах.

8. Оператор:

*а)* *государственный* *орган,* *муниципальный* *орган,* *юридическое* *или* *физическое* *лицо,* *самостоятельно* *или* *совместно* *с* *другими* *лицами* *организующие* *и* *(или)* *осуществляющие* *обработку* *персональных* *данных,* *а* *также* *определяющие* *цели* *обработки* *персональных* *данных,* *состав* *персональных* *данных,* *подлежащих* *обработке,* *действия* *(операции),* *совершаемые* *с* *персональными* *данными;*

б) юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных;

в) юридическое или физическое лицо, получившее на основании закона или договора право разрешать или ограничивать доступ к персональным данным.

9. Контроль над выполнением требований в сфере защиты персональных данных выполняют:

а)ФСБ РФ;

б) ФСТЭК России и Роскомнадзор;

*в)* *все* *перечисленные* *организации.*

10. За несоблюдение положений закона 152-ФЗ «О персональных данных» предусматривается:

а) гражданская, уголовная, административная ответственность; б) дисциплинарная и другие виды ответственности;

*в)* *все* *перечисленные* *виды* *ответственности.*

11. Блокирование персональных данных:

*а)* *временное* *прекращение* *обработки* *персональных* *данных;*

б) действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

в)действия, в результате которыхстановится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

12. Обезличивание персональных данных:

*а)* *действия,* *в* *результате* *которых* *становится* *невозможным* *без* *использования* *дополнительной* *информации* *определить* *принадлежность* *персональных* *данных* *конкретному* *субъекту* *персональных* *данных;*

б) действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных;

в) все перечисленные действия.

13. Срок хранения персональных данных в форме, позволяющей определить субъекта персональных данных:

а) 1 год;

б) 5 лет;

*в)* *не* *дольше,* *чем* *этого* *требуют* *цели* *обработки* *персональных* *данных,* *если* *иное* *не* *установлено* *законом* *или* *договором.*

14. Какую роль играют центры сертификации ключей:

а) они играют роль доверенной третьей стороны для доказывания факта передачи информации;

*б)* *они* *служат* *для* *регистрации* *абонентов,* *изготовления* *сертификатов* *открытых* *ключей,* *хранения* *изготовленных* *сертификатов,* *поддержания* *в* *актуальном* *состоянии* *справочника* *действующих* *сертификатов* *и* *выпуска* *списка* *досрочно* *отозванных* *сертификатов;*

в) они выдают сертификат соответствия длины сгенерированных ключей требованиям нормативных документов.

15. Использование электронной подписи позволяет не допустить (лишнее исключить):

а) отказ от авторства;

б) приписывание авторства;

*в)* *несанкционированное* *ознакомление* *с* *подписанным* *документов.*

16. Обязано ли лицо, осуществляющее обработку персональных данных по поручению оператора, получать согласие субъекта персональных данных на обработку его персональных данных:

*а)* *не* *обязано;*

б) обязано;

в) не обязано только в случаях, предусмотренных законом.

17. В общедоступные источники персональных данных (в том числе справочники, адресные книги) персональные данные включаются:

*а)* *с* *письменного* *согласия* *субъекта* *персональных* *данных;*

б) согласия субъекта персональных данных не требуется;

в) согласия субъекта персональных данных не требуется, но по требованию субъекта данные в любое время должны быть исключены из общедоступных источников персональных данных.

18. В общем случае, согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в:

а) только письменной форме;

*б)* *любой,* *позволяющей* *подтвердить* *факт* *его* *получения* *форме;*

в) устной форме.

19. При проведении контроля за выполнением организационных и технических мер по обеспечению безопасности персональных данных, при обработке персональных данных в государственных информационных системах персональных данных регуляторы:

а) вправе знакомиться с персональными данными, обрабатываемыми в информационных системах персональных данных;

*б)* *не* *вправе* *знакомиться* *с* *персональными* *данными,* *обрабатываемыми* *в* *информационных* *системах* *персональных* *данных;*

в) вправе знакомиться с персональными данными, обрабатываемыми в информационных системах персональных данных, только в установленных законом случаях.

20. Оператор обязан сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение:

*а)* *тридцати* *дней* *с* *даты* *получения* *такого* *запроса;*

б) десяти дней с даты получения такого запроса;

в) трех дней с даты получения такого запроса.

21. В случае достижения цели обработки персональных данных, если иное не предусмотрено договором, оператор обязан:

а) прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора);

б) уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора);

*в)* *все* *перечисленное.*

22. В случаях, когда необходимо уведомить уполномоченный орган по защите прав субъектов персональных данныхо своемнамеренииосуществлять обработку персональных данных, уведомление направляется:

*а)* *до* *начала* *обработки;*

б) в течении тридцати дней с момента начала обработки;

в) в течении десяти дней с момента начала обработки.

23. Субъект персональных данных:

а) имеет право на доступ к своим персональным данным во всех случаях;

б) не имеет право на доступ к своим персональным данным;

*в)* *имеет* *право* *на* *доступ* *к* *своим* *персональным* *данным* *за* *исключением* *случаев,* *предусмотренных* *законом.*

24. Контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности персональных данных, при обработке персональных данных в государственных информационных системах осуществляются:

а*)* *ФСТЭК* *России* *и* *ФСБ* *России;*

б) ФСТЭК России и органами Роскомнадзора;

в) ФСБ России и органами Роскомнадзора.

25. Какой нормативный акт является основным в сфере регулирования электронной подписи:

а) федеральный закон №1-ФЗ от 10.01.2002 «Об электронной цифровой подписи»;

*б)* *федеральный* *закон* *№63-ФЗ* *от* *06.04.2011* *«Об* *электронной* *подписи»;*

в) постановление Правительства Российской Федерации № 111 от 9 февраля 2012 г. «Об электронной подписи, используемой органами исполнительной власти и органами местного самоуправления при организации электронного взаимодействия между собой».

26. Перечислите виды электронной подписи:

а) простая, сложная, комбинированная;

б) простая, квалифицированная, сложная;

*в)* *простая,* *квалифицированная,* *неквалифицированная.*

27. СТР-К при защите государственных систем, обрабатывающих ПДн:

а) применяется в полном объеме;

б) не применяется;

*в)* *применяется* *при* *реализации* *мер* *по* *защите* *технических* *средств* *государственных* *информационных* *систем.*

28. Распространение аттестата соответствия на другие сегменты информационной системы:

*а)* *допускается* *при* *условии* *их* *соответствия* *сегментам* *информационной* *системы,* *прошедшим* *аттестационные* *испытания;*

б) допускается по решению оператора с оформлением акта;

в) не допускается.

29. Для обеспечения безопасности ПДн при их обработке в ИСПДн осуществляется защита:

а) речевой информации и информации, обрабатываемой техническими средствами, а также информации, представленной в виде информативных электрических сигналов;

б) физических полей, носителей на бумажной, магнитной, оптической и иной основе, в виде информационных массивов и баз данных в ИСПДн;

*в)* *всех* *видов* *информации.*

30. Идентификация это:

а) процесс предъявления пользователем идентификатора;

б) процесс подтверждения подлинности;

*в)* *сравнение* *предъявляемых* *идентификаторов* *с* *перечнем* *присвоенных* *идентификаторов.*

31. Что является организационной формой защиты информации:

а)разработка иреализация специальныхзаконов,нормативно-правовыхактов, правил и юридических процедур, обеспечивающих правовую защиту информации;

*б)* *регламентация* *производственной* *деятельности* *и* *взаимоотношений*

*персонала,* *направленная* *на* *защиту* *информации;*

в) использование различных технических, программных и аппаратных средств защиты информации от несанкционированного доступа, копирования, модификации или уничтожения.

32. Что является правовой формой защиты информации:

*а)* *разработка* *и* *реализация* *специальных* *законов,* *нормативно-правовых* *актов,* *правил* *и* *юридических* *процедур,* *обеспечивающих* *правовую* *защиту* *информации;*

б) регламентация производственной деятельности и взаимоотношений персонала, направленная на защиту информации;

в)использование различных технических, программных иаппаратных средств защитыинформацииот несанкционированногодоступа, копирования, модификации или уничтожения.

33. Что является инженерно-технической формой защиты информации:

а)разработка иреализация специальныхзаконов,нормативно-правовыхактов, правил и юридических процедур, обеспечивающих правовую защиту информации;

б) регламентация производственной деятельности и взаимоотношений

персонала, направленная на защиту информации;

*в)* *использование* *различныхтехнических,* *программных* *иаппаратных* *средств* *защиты* *информации* *от* *несанкционированного* *доступа,* *копирования,* *модификации* *или* *уничтожения.*

34. К числу определяющих признаков, по которым производится классификация информационных систем, относятся:

а) наличие в информационной системе информации различного уровня конфиденциальности;

*б)* *уровень* *значимости* *информации* *и* *масштаб* *информационной* *системы;* в) режим обработки данных в информационной системе - коллективный или индивидуальный.

35. Для ИСПДн устанавливается:

а) два уровня защищенности персональных данных; б) три уровня защищенности персональных данных;

*в)* *четыре* *уровня* *защищенности* *персональных* *данных.*

36. Замысел защиты информации:

*а)* *основная* *идея,* *раскрывающая* *состав,* *содержание,* *взаимосвязь* *и* *последовательность* *осуществления* *технических* *и* *организационных* *мероприятий,* *необходимых* *для* *достижения* *цели* *защиты* *информации;*

б) деятельность по обеспечению защиты не криптографическими методами информации от ее утечки по техническим каналам, от несанкционированного доступа к ней, от специальных воздействий на информацию;

в) совокупность объекта защиты, физической среды и средства технической разведки, которым добывается защищаемая информация.

37. Для государственной информационной системы проводится: а) классификация ИС;

б) определение уровня защищенности ПДн;

*в)* *классификация* *ИС* *и* *определение* *уровня* *защищенности* *ПДн.*

38. Оценка эффективности реализованных мер по защите ПДн в государственных ИС:

*а)* *проводится* *в* *рамках* *обязательной* *аттестации* *государственной* *информационной* *системы* *по* *требованиям* *защиты* *информации;*

б) проводиться оператором самостоятельно в рамках мероприятий по контролю;

в) форма оценки эффективности, а также форма и содержание документов, разрабатываемых по результатам (в процессе) оценки, ФСТЭК России не установлены.

39. Уровень защищенности ПДн устанавливается в зависимости от: а) типа угроз, актуальных для ИСПДн и категории обрабатываемых ПДн; б) объема ПДн, обрабатываемых в ИСПДн;

*в)* *типа* *угроз,* *актуальных* *для* *ИСПДн,* *категории* *обрабатываемых* *ПДн,* *объема* *ПДн,* *обрабатываемых* *в* *ИСПДн.*

40. Средства защиты информации:

*а)* *должны* *проходить* *контроль* *на* *отсутствие* *недекларированных возможностей;*

б) не должны проходить контроль на отсутствие недекларированных возможностей;

в) должны проходить контроль на отсутствие недекларированных возможностей по усмотрению оператора.

41. Системное программное обеспечение:

а) проходит контроль на отсутствие недекларированных возможностей;

б) не проходит контроль на отсутствие недекларированных возможностей;

*в)* *проходит* *контроль* *на* *отсутствие* *недекларированных* *возможностей* *по* *усмотрению* *оператора.*

42. Прикладное программное обеспечение:

а) проходит контроль на отсутствие недекларированных возможностей;

б) не проходит контроль на отсутствие недекларированных возможностей;

*в)* *проходит* *контроль* *на* *отсутствие* *недекларированных* *возможностей* *по* *усмотрению* *оператора.*

43. Аттестацию информационных систем по требованиям безопасности информации:

а) оператор проводит самостоятельно, с привлечением штатных специалистов по защите информации;

*б)* *проводит* *орган* *по* *аттестации,* *аккредитованный* *ФСТЭК* *России;* в) государственные информационные системы не подлежат аттестации.

44. Что относится к основным механизмам защиты компьютерной системы от несанкционированного доступа:

*а)* *физическая* *защита* *компонент* *компьютерной* *системы,* *идентификация* *и* *аутентификация,* *разграничение* *доступа,* *контроль* *обращений* *к* *защищаемой* *информации;*

б) дублирование информации, создание отказоустойчивых компьютерных систем, блокировка ошибочных операций, повышение надежности компьютерных систем;

в) сегментация сетей с помощью коммутаторов и межсетевых экранов, шифрование информации.

45. Какие основные способы разграничения доступа применяются в компьютерных системах:

*а)* *дискреционный* *и* *мандатный;*

б) по специальным спискам и многоуровневый;

в) по группам пользователей и специальным разовым разрешениям.

46. Кто должен анализировать журнал аудита безопасности компьютерной системы:

а) администратор; *б)* *аудитор;*

в) начальник.

47. Аутентификация это:

а) процесс предъявления пользователем идентификатора; *б)* *процесс* *подтверждения* *подлинности;*

в) регистрация всех обращений к защищаемой информации.

48. Какие основные компоненты входят в состав удостоверяющего центра:

а) центр сертификации, центр авторизации, АРМ администратора; б) центр регистрации, центр авторизации, АРМ администратора;

*в)* *центр* *сертификации,* *центр* *регистрации,* *АРМ* *администратора.*

49. Что собой представляет сертификат электронного ключа подписи:

*а)* *это* *электронный* *документ* *или* *документ* *на* *бумажном* *носителе,* *выданные* *удостоверяющим* *центром* *либо* *доверенным* *лицом* *удостоверяющего* *центра* *и* *подтверждающие* *принадлежность* *ключа* *проверки* *ЭП* *владельцу* *сертификата* *ключа* *проверки* *ЭП;*

б) это документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки ЭП владельцу сертификата ключа проверки ЭП;

в) это логическая посимвольная свертка подписываемого сообщения, зашифрованная на открытом ключе получателя.

50. Перечислите основные компоненты программного комплекса ViPNet CUSTOM:

*а)* *client,* *administrator,* *coordinator;*

б) client, administrator, certificate center;

в) administrator, coordinator, certificate center.

1. **Формы аттестации**

Оценка результатов освоения слушателями программы проводится в форме итоговой аттестации на основе 100 бальной системы оценивания.

Для оценки освоения отдельных модулей программы, а также при проведении итоговой аттестации используются система «зачет» и «незачет» в соответствии с критериями оценивания, указанными в настоящей программе.

Промежуточная аттестация:

Предусматривает проверку знаний после завершения изучения соответствующего раздела программы и проводится в форме собеседования.

Итоговая аттестация:

Итоговая аттестация осуществляется после освоения всех учебных разделов программы. Итоговая аттестация предусматривает экзамен в форме тестирования.

Итоговая аттестация проводится экзаменационной комиссией, которая оценивает результат выполнения итогового теста как одного из главных показателей эффективности обучения слушателей и принимает решение о выдаче слушателям, успешно освоившим программу и прошедшим итоговую аттестацию, удостоверения о повышении квалификации.

Лицам, не прошедшим итоговой аттестации или получившим на итоговой аттестации неудовлетворительные результаты, а также лицам, освоившим часть программы и (или) отчисленным из Академии госслужбы выдается справка об обучении или о периоде обучения.

Критерии оценивания.

Оценка «зачтено» на итоговой аттестации ставится в случае, если набрано не менее 50 баллов из 100 возможных.

Программа считается освоенной, если успешно освоены все учебные разделы и успешно пройдена итоговая аттестация.