Программа повышения квалификации

«ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ при их обработке в информационных системах персональных данных», 72 часа

(согласовано ФСТЭК)

Модуль 1. Общие вопросы технической защиты информации

Тема 1.1. Правовые и организационные вопросы технической защиты информации ограниченного доступа

- Основные понятие в области технической защиты информации (ТЗИ). Стратегия национальной безопасности РФ до 2030 г. Доктрина информационной безопасности РФ. Актуальные ГОСТы.
- Понятия методов, способов и средств защиты информации
- Организация комплексных организационно-технических мероприятий защиты персональных данных (ПДн). Правила обработки и обеспечения безопасности ПДн.
- Разработка необходимых форм учета.
- Концептуальные основы ТЗИ. Законодательные и иные правовые акты, регулирующие вопросы ТЗИ. Система документов по ТЗИ и краткая характеристика ее основных составляющих.
- Государственные регуляторы в области защиты информации.
- Нормативные документы, регламентирующие вопросы защиты информации в информационных системах.
- Актуальные изменения в ФЗ-152 «О персональных данных».
- Критерии ПДн и уровни защищенности ПДн.
- Организация оператором ПДн контроля за выполнением требований к защите ПДн при их обработке в ИС ПДн.
- Состав мер по обеспечению безопасности ПДн с учетом актуальных угроз безопасности ПДн.
- Уровни защищенности ПДн.
- Порядок определения мер защиты информации.
- Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах». Нормативные правовые акты ФСБ России.
- Ответственность за нарушение законодательства Российской Федерации в области ПДн.

Тема 1.2. Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа

- Понятие «безопасности информации», «угрозы безопасности информации», «уязвимости», «источника угрозы». ГОСТы. Целостность, конфиденциальность и доступность информации.
- Необходимость определения угроз безопасности информации.
- Классификационная схема угроз безопасности информации и их общая характеристика.
- Особенности проведения комплексного исследования объектов информатизации на наличие угроз безопасности информации. Методика оценки угроз безопасности информации.
- Основные задачи, решаемые в ходе оценки угроз безопасности информации.
- Оценка возможности реализации мероприятий по УБИ.
- Банк данных угроз ФСТЭК России.
- Модель угроз в 7 шагов.
- Классификация объектов информатизации. Методические рекомендации по классификации и категорированию объектов информатизации. Характеристика основных угроз несанкционированного доступа и моделей нарушителя безопасности информации, а также способов реализации этих угроз. Характеристика основных классов атак,

реализуемых в сетях общего пользования, функционирующих с использованием стека протоколов TCP/IP. Понятие программно-математического воздействия вредоносной программы.

- Классификация вредоносных программ, основных деструктивных функций вредоносных программ и способов реализации. Особенности программно-математического воздействия в сетях общего пользования. Методы и средства выявления угроз несанкционированного доступа и специальных воздействий на нее. Порядок обеспечения защиты информации при эксплуатации автоматизированных систем.
- Зашита информации на автоматизированных рабочих местах на базе автономных ПЭВМ. Защита информации в локальных вычислительных сетях. Защита информации при межсетевом взаимодействии. Защита информации при работе с системами управления базами данных. Порядок обеспечения защиты информации при взаимодействии с информационными сетями общего пользования.
- Требования и рекомендации по защите информации, обрабатываемой средствами вычислительной техники.
- Содержание и порядок проведения аттестации объектов информатизации по требованиям безопасности информации. Структура, содержание и порядок подготовки документов при аттестации объектов информатизации по требованиям безопасности информации.

Модуль 2. Организация обеспечения безопасности ПДн в ИС ПДн

Тема 2.1. Угрозы безопасности ПДн при их обработке в информационных системах (ИС) ПДн, организационные и технические меры защиты информации в ИС ПДн

- Особенности информационного элемента информационных системах ПДн.
- Основные типы актуальных угроз безопасности ПДн при их обработке в информационных в ИС ПДн, порядок их определения. Угрозы несанкционированного доступа к информации в ИС ПДн. Угрозы утечки информации по техническим каналам.
- Основные принципы обеспечения безопасности ПДн при их обработке: законности, превентивности, адекватности, непрерывности, адаптивности, самозащиты, многоуровневости, персональной ответственности и минимизации привилегий, разделения полномочий и их характеристика. Основные направления деятельности по обеспечению безопасности ПДн при их обработке в ИС ПДн. Общий порядок организации обеспечения безопасности ПДн в ИС ПДн. Оценка достаточности и обоснованности запланированных мероприятий.
- Особенности обеспечения безопасности ПДн, обрабатываемых на автоматизированных рабочих местах с использованием ПЭВМ, в локальных вычислительных сетях и при межсетевом взаимодействии.
- Рекомендации по применению мер и средств обеспечения безопасности ПДн от физического доступа.
- Причины и физические явления, порождающие технические каналы утечки информации (ТКУИ) при эксплуатации объектов информатизации. Классификация ТКУИ.
- Основные требования и рекомендации по защите речевой информации, циркулирующей в защищаемых помещениях.
- Оценка защищенности информации, обрабатываемой основными техническими средствами и системами, от утечки за сет наводок на вспомогательные технические средства и системы их коммуникации.

Тема 2.2. Основы организации и ведения работ по обеспечению безопасности ПДн при их обработке в ИС ПДн

- Определение необходимых уровней защищенности ПДн при их разработке в информационных системах в зависимости от типа актуальных угроз для информационных систем, вида и объема обрабатываемых в них ПДн.
- Состав мер по обеспечению безопасности ПДн, реализуемых в рамках системы защиты ПДн с учетом актуальных угроз безопасности ПДн и применяемых информационных технологий.

- Порядок выбора мер по обеспечению безопасности ПДн, подлежащих реализации в информационной системе в рамках системы защиты ПДн: определение базового набора мер, адаптация базового набора, уточнение адаптированного базового набора мер, дополнение уточненного адаптированного базового набора мер.
- Содержание мер по обеспечению безопасности ПДн, реализуемых в рамках системы защиты ПДн.
- Требования к средствам защиты информации для обеспечения различных уровней защищенности ПДн.
- Средства аппаратной аутентификации. Идентификация и аутентификация субъектов доступа.
- Управление доступом субъектов доступа к объектам доступа.
- Средства защиты информации от НСД.
- Антивирусная защита.
- Средства обнаружения вторжения уровня сети и хоста.
- Средства контроля (анализа) защищенности информации.
- Организация обеспечения безопасности ПДн в организациях и учреждениях. Перечень основных этапов при организации работ по обеспечению безопасности ПДн.
- Мероприятия по техническому обеспечению безопасности ПДн при их обработке в ИС ПДн и особенности их реализации.
- Содержание, порядок разработки и ввода в действие внутренних нормативных документов и актов ненормированного характера по обработке ПДн и обеспечению безопасности ПДн. Подготовка уведомлений об обработке ПДн в уполномоченный орган, порядок внесения изменений в ранее представленное в уполномоченный орган уведомление.
- Обязанности оператора, осуществляющего обработку ПДн. Порядок и методы обезличивания ПДн, их дезобличивание. Особенности обработки ПДн в условиях государственной гражданской службы и муниципальной службы. Ответственность за нарушение требований законодательства РФ в области ПДн.

Тема 2.3. Практические реализации типовых моделей защищенных ИС обработки ПДн

- Комплекс организационных и технических мероприятий (применения технических средств), в рамках подсистемы защиты ПДн, развертываемой в ИС ПДн в процессе ее создания или модернизации. Основное содержание этапов организации обеспечения безопасности ПДн.
- Варианты реализации мероприятий по защите ПДн и типовые модели защищенных ИС ПДн с использованием существующих сертифицированных средств защиты информации.
- Стадии и этапы разработки систем защиты информации. Аналитическое обоснование необходимости создания системы защиты информации информационной системы. Разработка технического задания на систему защиты информации информационной системы. Разработка и оформление документации на систему защиты информации информационной системы.
- Виды, формы и способы контроля защиты ПДн в ИС ПДн. Планирование работ по контролю состояния защиты ПДн в ИС ПДн. Основные вопросы, подлежащие проверке (анализу) при контроле состояния организации защиты ПДн.
- Оценка эффективности реализованных в рамках системы защиты ПДн мер по обеспечению безопасности ПДн. Аттестация объектов информатизации по требованиям безопасности информации.
- Объекты информатизации, аттестуемые по требованиям безопасности информации.
- ГОСТ РО-003-2012 (ДСП).
- Функции ФСТЭК России.
- Функции, права и обязанности органа по аттестации.
- Программа и методики аттестационных испытаний.
- Аттестат соответствия для государственных информационных систем.
- Эксплуатация аттестованного объекта информатизации.