**Перечень работ и разрабатываемых документов по обеспечению безопасности персональных данных (ПДн) при их обработке в информационных системах персональных данных (ИСПДн).**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п.п.** | **Перечень выполняемых мероприятий и работ** | **Основание** | **Наименование отчетных документов** |
| **1.** | **Предварительное обследование информационной системы обработки персональных данных (ИСПДн)** | | |
| 1.1. | Разработка перечня ПДн, подлежащих защите от НСД в ИСПДн. | 1. Перечень сведений конфиденциального характера, утвержден указом Президента РФ № 188 от 6 марта 1997 г. 2. ФЗ-152 «О персональных данных» | Перечень ПДн, подлежащих защите от НСД в ИСПДн |
| 1.2. | Определение уровня защищенности персональных данных. | 1. п.5, 8 Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» | 1. Приказ о назначении комиссии по определению уровня защищенности ИСПДн. 2. Акт определения уровня защищенности ИСПДн. |
| 1.3. | Согласие субъекта ПДн на обработку | ФЗ-152«О персональных данных» | Письменное согласие субъекта ПДн на обработку (договор) |
| 1.4. | Назначение структурного подразделения или должностного лица, ответственных за обеспечение безопасности ПДн | 1. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» 2. п. 14 Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» | 1. Приказ о назначении. 2. Инструкция ответственному за обеспечение безопасности ПДн |
| 1.5. | Разработка документации по обеспечению безопасности ПДн | 1. ФЗ-152 «О персональных данных» 2. Трудовой кодекс | 1. Положение о порядке организации и проведения работ по обеспечению безопасности ПДн при их обработке в ИСПДн. 2. Положение об обработке ПДн. 3. Обязательство о неразглашении конфиденциальной информации |
| 1.6. | Организация режима обеспечения безопасности помещений, в которых размещена информационная система | 1. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» 2. п.13 Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» | * + - 1. Положение о разрешительной системе доступа.       2. Список лиц, допущенных к обработке ПДн.       3. Матрица доступа.       4. Должностные инструкции пользователей ИСПДн. |
| 1.7. | Организация учета и хранения съемных носителей информации и их обращение | 1. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» 2. п.13 Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» | * + - 1. Журнал учета и хранения съемных носителей информации.       2. Положения… – см. п. 1.5. |
| **2** | **Выбор методов, средств и способов защиты информации в ИСПДн** | | |
| 2.1. | Анализ технических средств и систем, используемых в ИСПДн, условия их расположения, общесистемных и прикладных программных средств. | 1. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» 2. ГОСТ Р 53109-2008. Система обеспечения информационной безопасности сети связи общего пользования. паспорт организации связи по информационной безопасности. 3. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). | 1. Схема расположения ИСПДн относительно границ контролируемой зоны. 2. Топологическая схема ИСПДн с физическими, функциональными и технологическими связями |
| 2.2. | Определение режимов обработки ПДн в ИСПДн в целом и в отдельных компонентах. | 1. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» | * + - 1. Описание технологического процесса обработки ПДн       2. Схема информационных потоков |
| 2.3. | Определение угроз безопасности ПДн к конкретным условиям функционирования. | 1. п.6 Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»  2. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, ФСТЭК, 2008 г.  3. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», ФСТЭК, 2008 г.  4. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации. ФСБ, 21 февраля 2008 г. | Частная модель угроз |
| 2.4 | Разработка замысла обеспечения безопасности ПДн (предотвращение несанкционированного физического доступа, программные и программно-аппаратные меры и средства обеспечения безопасности, межсетевое экранирование). | 1. Указ Президента РФ от 17 марта 2008 г. № 351 "О мерах по обеспечению информационной безопасности РФ при использовании информационно-телекоммуникационных сетей международного информационного обмена" 2. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» 3. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). | 1. Аналитическое обоснование создания СЗПДн. 2. Техническое задание на проектирование (модернизацию) подсистем информационной безопасности. 3. Технический проект (частное техническое задание). |
| 2.5 | Определение базового (компенсирующего) набора мер по обеспечению безопасности персональных данных для установленного уровня защищенности персональных данных.  Выбор средств защиты информации, прошедших процедуру оценки соответствия  Разработка технического проекта на СЗПДн | 1. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» 2. п.13 Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» 3. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). 4. ГОСТ 51624-00. Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. 5. ГОСТ 50752-95. Средства вычислительной техники. Защита от НСД к информации. Общие технические требования. 6. ГОСТ 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. 7. РД «Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от несанкционированного доступа». 8. РД «Средства вычислительной техники. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации». 9. РД «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля недекларированных возможностей» |
| **3** | **Реализация методов, средств и способов защиты информации в ИСПДн** | | |
| 3.1 | Проектирование и монтаж системы контроля управления доступом и системы охранно-пожарной сигнализации, помещений, в которых ведется работа с ПДн, организация режима обеспечения безопасности в этих помещениях. | 1. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». 2. Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» | 1. Акты установки и монтажа. 2. Эксплуатационная документация. 3. Инструкции по эксплуатации. |
| 3.1. | Установка и настройка сертифицированных средств защиты информации. | 1. п. 4 Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». 2. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). | 1. Акты установки и монтажа. 2. Сертификаты соответствия требованиям безопасности. 3. Эксплуатационная документация. 4. Инструкции по эксплуатации. |
| 3.2. | Разработка организационно-распорядительная документации (действия администраторов и пользователей, порядок контроля за соблюдением условий использования СЗИ и т.д.). | Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). | 1. Должностные инструкции персоналу ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн; 2. Рекомендации (инструкции) по использованию программных и аппаратных средств защиты информации. |
| 3.4. | Учет лиц, допущенных к работе с персональными данными в информационной системе. | Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». | Распоряжение руководителя организации о допуске лиц к работе с персональными данными. |
| 3.6. | Уведомление Ростехнадзора (при необходимости) | 1. Статья 22ФЗ-152 «О персональных данных» | Уведомление |
| **4.** | **Оценка соответствия ИСПДн требованиям безопасности информации (Аттестационные испытания информационных систем обработки персональных данных (ИСПД) по требованиям безопасности информации)**  п. 6 Приказа ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».  п.17 Постановления Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» | | |
| 4.1 | Подача заявки на проведение аттестации ИСПДн | Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). | Договор об оказании услуг в области персональных данных. |
| 4.2. | Оценка мероприятий по защите от НСД к ПДн при их обработке в ИСПДн:   * + управление доступом;   + регистрацию и учет;   + обеспечение целостности;   + контроль отсутствия недекларированных возможностей;   + антивирусную защиту;   + обеспечение безопасного межсетевого взаимодействия ИСПДн;   + анализ защищенности;   + обнаружение вторжений. | Документы ФСТЭК:   1. РД «Аттестационные испытания АС по требованиям безопасности информации. Типовая методика испытаний объектов информатики по требованиям безопасности информации (Аттестация АС)». 2. РД «Положение по аттестации объектов информатизации по требованиям безопасности информации». 3. ГОСТ Р 50752-95. Информационная технология. Защита информации от утечки за счет побочных электромагнитных излучений при ее обработке средствами вычислительной техники. Методы испытаний; 4. ГОСТ Р 29339-92. Информационная технология. Защита информации от утечки за счет побочных электромагнитных излучений при ее обработке средствами вычислительной техники. Общие технические требования; 5. Сборник норм защиты информации от утечки за счет побочных электромагнитных излучений и наводок (ПЭМИН). Гостехкомиссия России, 1998 г.; 6. Сборник методических документов по контролю защищенности информации, обрабатываемой средствами вычислительной техники, от утечки за счет побочных электромагнитных излучений и наводок (ПЭМИН). Утвержден приказом ФСТЭК России от 30 декабря 2005 г. 7. «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», Гостехкомиссия России, 1992 г. 8. «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности СВТ», Гостехкомиссия России, 1992 г. 9. ГОСТ 51624-00. Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. 10. ГОСТ 50752-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. 11. ГОСТ 50922-96. Защита информации. Основные требования и определения. 12. ГОСТ 51188-98. Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство. 13. ГОСТ 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. 14. «Программа-методика аттестационных испытаний объектов информатизации автоматизированного рабочего места | Протокол проверки выполнения требований по защите информации от несанкционированного доступа |
| 4.3 | Оценка мероприятий по защите информации от утечки по техническим каналам:   * + Проверка соответствия СВТ требованиям стандартов РФ по электромагнитной совместимости, по безопасности и эргономическим требованиям к средствам отображения информации, по санитарным нормам, предъявляемым к видеодисплейным терминалам ПЭВМ;   + нарушений безопасности функционирования ИСПДн и СЗПДн от угроз неатропогенного характера.   + Оценка размещения средств вычислительной техники с точки зрения защищенности ПДн от утечки по оптическому каналу. |
| 4.4 | Подготовка отчетных документов | * + 1. Протокол аттестационных испытаний     2. Предписание на эксплуатацию ТС.     3. Предписание на эксплуатацию ОВТ.     4. Заключение по результатам испытаний.     5. Аттестат соответствия требованиям информационной безопасности.     6. Технический паспорт АРМ (ИСПДн) |
| **5.** | **Сопровождение системы защиты персональных данных** | | |
| 5.1 | Контроль обеспечения безопасности персональных данных в организационной и технической части |  | 1. Отчеты о плановых мероприятиях, описывающих актуальное состояние систем защиты персональных данных. 2. Возможность оперативно реагировать на изменение системы защиты персональных данных. 3. Постоянную готовность к проверкам регулирующих органов. |
| 5.2 | Ведение электронного журнала сообщений | п.15 Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» |  |
| 5.3 | Ведение электронного журнала безопасности | п.16 Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» |  |