Заместитель начальника отдела специальных экспертиз
Управления ФСТЭК России
по Приволжскому федеральному округу,
кандидат технических наук

МОКЛЯКОВ
Виталий Александрович

ЗАКОНОДАТЕЛЬНАЯ БАЗА ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Федеральный закон N 152-ФЗ от 27 июля 2006 г.

"О персональных данных"

Постановление Правительства РФ от 17 ноября 2007 г. № 781

«Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»,

«Порядок проведения классификации информационных систем персональных данных»

Утвержден приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 г. № 55/86/20.

ЗАКОНОДАТЕЛЬНАЯ БАЗА ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

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

Утверждены ФСТЭК России 14 февраля 2008 г.

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

Утверждены ФСТЭК России 15 февраля 2008 г.

«Основные мероприятия по организации и техническому обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

Утверждены ФСТЭК России 15 февраля 2008 г.

«Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

Утверждены ФСТЭК России 15 февраля 2008 г.

Документы, разработанные ФСБ России во исполнение Федерального закона № 152-ФЗ «О персональных данных» и Постановления Правительства Российской Федерации от 17 ноября 2007 г. № 781

- «**Методические рекомендации** по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации»
- «**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»

ЗАКОНОДАТЕЛЬНАЯ БАЗА ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Федеральный закон Российской Федерации от 27 декабря 2009 г. N 363-ФЗ

"О внесении изменений в статьи 19 и 25 Федерального закона "О персональных данных«

Внести в Федеральный закон от 27 июля 2006 года N 152-ФЗ "О персональных данных" (Собрание законодательства Российской Федерации, 2006, N 31, ст. 3451) следующие изменения:

1) в части 1 статьи 19 слова ", в том числе использовать шифровальные (криптографические) средства," исключить;

2) часть 3 статьи 25 изложить в следующей редакции:

"3. Информационные системы персональных данных, созданные до 1 января 2010 года, должны быть приведены в соответствие с требованиями настоящего Федерального закона не позднее 1 января 2011 года.".

ПОЛОЖЕНИЕ

о методах и способах защиты информации в информационных системах персональных данных

Утверждено приказом ФСТЭК России 5 февраля 2010г. № 58

Зарегистрирован в Минюсте РФ 19 февраля 2010 г.

Регистрационный N 16456

Федеральный закон N 152-ФЗ от 27 июля 2006 г. "О персональных данных"

Оператор при обработке персональных данных

обязан принимать необходимые организационные и технические меры,

для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

Статья 19, п.1

Положение о методах и способах защиты информации в информационных системах персональных данных

1.3. Для выбора и реализации методов и способов защиты информации в информационной системе оператором или уполномоченным лицом может назначаться структурное подразделение или должностное лицо (работник), ответственные за обеспечение безопасности персональных данных.

Для выбора и реализации методов и способов защиты информации в информационной системе может привлекаться организация, имеющая оформленную в установленном порядке лицензию на осуществление деятельности по технической защите конфиденциальной информации.

Положение о методах и способах защиты информации в информационных системах персональных данных

1.4. Выбор и реализация методов и способов защиты информации в информационной системе осуществляются на основе определяемых оператором (уполномоченным лицом) угроз безопасности персональных данных (модели угроз) и в зависимости от класса информационной системы, определенного в соответствии с Порядком проведения классификации информационных систем персональных данных, утвержденным приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 г. N 55/86/20.

Модель угроз разрабатывается на основе методических документов, утвержденных в соответствии с пунктом 2 постановления Правительства Российской Федерации от 17 ноября 2007 г. N 781.

КЛАСС ТИПОВОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Хнпд / Хпд	3 <1000	2 1000 до 100 000	1 >100 000
категория 4	К4	К4	К4
категория 3	К3	К3	К2
категория 2	К3	К2	К1
категория 1	К1	К1	К1

Порядок проведения классификации информационных систем персональных данных

Категории обрабатываемых в информационной системе персональных данных – Хпд

- категория 1 - персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;
- категория 2 - персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1;
- категория 3 - персональные данные, позволяющие идентифицировать субъекта персональных данных;
- категория 4 - обезличенные и (или) общедоступные персональные данные.

«Порядок проведения классификации информационных систем персональных данных»

В зависимости от объема Хнпд может принимать следующие значения:

1. - в информационной системе одновременно обрабатываются персональные данные более чем 100 000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах субъекта Российской Федерации или Российской Федерации в целом;
2. - в информационной системе одновременно обрабатываются персональные данные от 1000 до 100 000 субъектов персональных данных или персональные данные субъектов персональных данных, работающих в отрасли экономики Российской Федерации, в органе государственной власти, проживающих в пределах муниципального образования;
3. - в информационной системе одновременно обрабатываются данные менее чем 1000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах конкретной организации.

КЛАСС ТИПОВОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

- класс 1 (К1) -информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к значительным негативным последствиям для субъектов персональных данных;
- класс 2 (К2) - информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к негативным последствиям для субъектов персональных данных;
- класс 3 (К3) -информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов персональных данных;
- класс 4 (К4) - информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, не приводит к негативным последствиям для субъектов персональных данных.

Порядок проведения классификации информационных систем персональных данных

Типовые информационные системы

- информационные системы, в которых требуется обеспечение только конфиденциальности персональных данных

Специальные информационные системы

- информационные системы, в которых вне зависимости от необходимости обеспечения конфиденциальности персональных данных требуется обеспечить хотя бы одну из характеристик безопасности персональных данных, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий)

МЕТОДИКА ОПРЕДЕЛЕНИЯ АКТУАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Под угрозами безопасности ПДн при их обработке в ИСПДн понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и (или) несанкционированными и (или) непреднамеренными воздействиями на нее.

БАЗОВАЯ МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Содержит систематизированный перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных (ИСПДн).

Эти угрозы обусловлены преднамеренными или непреднамеренными действиями физических лиц, действиями зарубежных спецслужб или организаций (в том числе террористических), а также криминальных группировок, создающими условия (предпосылки) для нарушения безопасности персональных данных (ПДн), которые ведут к ущербу жизненно важным интересам личности, общества и государства.

При оценке опасности на основе опроса экспертов (специалистов в области защиты информации) определяется вербальный показатель опасности для рассматриваемой ИСПДн.
Этот показатель имеет три значения:

низкая опасность - если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;

средняя опасность - если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;

высокая опасность - если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Для исключения утечки ПДн за счет ПЭМИН в ИСПДн 1 класса реализуются следующие мероприятия:

- использование сертифицированных серийно выпускаемых в защищенном исполнении технических средств;
- использование сертифицированных средств защиты информации;
- размещение объектов защиты на максимально возможном расстоянии относительно границы КЗ;
- размещение понижающих трансформаторных подстанций электропитания и контуров заземления объектов защиты в пределах КЗ;
- обеспечение развязки цепей электропитания объектов защиты с помощью защитных фильтров, блокирующих (подавляющих) информативный сигнал;
- обеспечение электромагнитной развязки между линиями связи и другими цепями ВТСС, выходящими за пределы КЗ, и информационными цепями, по которым циркулирует защищаемая информация.

ПОЛОЖЕНИЕ о методах и способах защиты информации в информационных системах персональных данных

3.2. Для исключения утечки персональных данных за счет побочных электромагнитных излучений и наводок в информационных системах 1 класса могут применяться следующие методы и способы защиты информации:

- **использование технических средств в защищенном исполнении;**
- **использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;**
- **размещение объектов защиты в соответствии с предписанием на эксплуатацию;**
- **размещение понижающих трансформаторных подстанций электропитания и контуров заземления технических средств в пределах охраняемой территории;**
- **обеспечение развязки цепей электропитания технических средств с помощью защитных фильтров, блокирующих (подавляющих) информативный сигнал;**
- **обеспечение электромагнитной развязки между линиями связи и другими цепями вспомогательных технических средств и систем, выходящими за пределы охраняемой территории, и информационными цепями, по которым циркулирует защищаемая информация.**

В ИСПДн 2 класса для обработки информации рекомендуется

использовать СВТ, удовлетворяющие требованиям стандартов Российской Федерации по электромагнитной совместимости, по безопасности и эргономическим требованиям к средствам отображения информации, по санитарным нормам, предъявляемым к видеодисплейным терминалам ПЭВМ (например, ГОСТ 29216-91, ГОСТ Р 50948-96, ГОСТ Р 50949-96, ГОСТ Р 50923-96, СанПиН 2.2.2.542-96).

ПОЛОЖЕНИЕ о методах и способах защиты информации в информационных системах персональных данных

3.3. В информационных системах 2 класса для обработки информации используются средства вычислительной техники, удовлетворяющие требованиям национальных стандартов по электромагнитной совместимости, по безопасности и эргономическим требованиям к средствам отображения информации, по санитарным нормам, предъявляемым к видеодисплейным терминалам средств вычислительной техники.

Оценка соответствия информационных систем персональных данных по требованиям безопасности

- для ИСПДн 1 и 2 классов - обязательная сертификация (аттестация) по требованиям безопасности информации;
- для ИСПДн 3 класса - декларирование соответствия требованиям безопасности информации;
- для ИСПДн 4 класса оценка соответствия проводится по решению оператора.

Дифференцированный подход к обеспечению безопасности персональных данных (оценка соответствия)

Класс ИСПДн	К1	К2	К3	К4
Оценка соответствия ИСПДн по требованиям безопасности ПДн	обязательная сертификация (аттестация) по требованиям безопасности информации		декларирование соответствия требованиям безопасности информации	оценка соответствия проводится по решению оператора
Последствия при нарушении заданной характеристики безопасности ПДн	значительные негативные последствия	негативные последствия	незначительные негативные последствия	не приводит к негативным последствиям

ФЕДЕРАЛЬНЫЙ ЗАКОН
О ТЕХНИЧЕСКОМ РЕГУЛИРОВАНИИ
от 27 декабря 2002 года N 184-ФЗ

1. Декларирование соответствия осуществляется по одной из следующих схем:

- **принятие декларации о соответствии на основании собственных доказательств;**
- **принятие декларации о соответствии на основании собственных доказательств, доказательств, полученных с участием органа по сертификации и (или) аккредитованной испытательной лаборатории (центра)**

Статья 24

ФЕДЕРАЛЬНЫЙ ЗАКОН
О ТЕХНИЧЕСКОМ РЕГУЛИРОВАНИИ
от 27 декабря 2002 года N 184-ФЗ

2. При декларировании соответствия на основании собственных доказательств заявитель самостоятельно формирует доказательственные материалы в целях подтверждения соответствия продукции требованиям технических регламентов.

В качестве доказательственных материалов используются техническая документация, результаты собственных исследований (испытаний) и измерений и (или) другие документы, послужившие мотивированным основанием для подтверждения соответствия продукции требованиям технических регламентов.

Статья 24

Документы для 3 класса

1. **Технический паспорт на ОИ**
2. **Протокол контроля соответствия ОИ требованиям по защите от НСД (экспертно-документальным методом и проведением необходимых спец. исследований).**
3. **Акты установки СЗИ с инструкциями на эксплуатацию.**
4. **Заключение по результатам испытаний ОИ**

Уведомление направлять в Управление
документы не прикладываются

Документы для 2 класса

1. Технический паспорт на ОИ
2. Программа и методики аттестационных испытаний
3. Протокол контроля соответствия ОИ требованиям по ПЭМИН (экспертно-документальным методом)
4. Протокол контроля соответствия ОИ требованиям по защите от НСД (экспертно-документальным методом и проведением необходимых спец. исследований).
5. Акты установки СЗИ с инструкциями на эксплуатацию.
6. Заключение по результатам аттестационных испытаний ОИ
7. Аттестат соответствия

Документы для 1 класса

1. Технический паспорт на ОИ
2. Программа и методики аттестационных испытаний
3. Предписание на эксплуатацию технических средств с приложением протокола контроля требованиям по ПЭМИН (специальные исследования) (Сертификат)
4. Протокол(ы) контроля соответствия ОИ требованиям по ПЭМИН (экспертно-документальным методом)
5. Протокол контроля соответствия ОИ требованиям по защите от НСД (экспертно-документальным методом и проведением необходимых спец. исследований).
6. Акты установки СЗИ с инструкциями на эксплуатацию.
7. Заключение по результатам аттестационных испытаний ОИ
8. Аттестат соответствия

ДОКУМЕНТЫ ПРЕДСТАВЛЯЕМЫЕ ОРГАНИЗАЦИЕЙ-ЗАЯВИТЕЛЕМ ДЛЯ ПРОВЕДЕНИЯ АТТЕСТАЦИОННЫХ ИСПЫТАНИЙ.

1. Техническое задание (ТЗ) на объект информатизации (ОИ).
2. Технический паспорт на ОИ.
3. Приемо-сдаточная документация на ОИ.
4. Акт классификации автоматизированных систем (АС) по требованиям защиты информации (ЗИ).
5. Состав технических и программных средств, входящих в АС (или технических средств (ТС), расположенных в ЗП).
6. Планы размещения основных технических средств и систем (ОТСС) и вспомогательных технических средств и систем (ВТСС).
7. Состав и схемы размещения средств защиты информации (СЗИ).
8. План контролируемой зоны (КЗ) предприятия.
9. Схемы прокладки линий передачи данных.
10. Схемы и характеристики систем электропитания и заземления ОИ.
11. Перечень защищаемых в АС ресурсов с документальным подтверждением степени конфиденциальности каждого ресурса (или максимальной степени конфиденциальности обсуждаемых в ЗП вопросов).

ДОКУМЕНТЫ ПРЕДСТАВЛЯЕМЫЕ ОРГАНИЗАЦИЕЙ-ЗАЯВИТЕЛЕМ ДЛЯ ПРОВЕДЕНИЯ АТТЕСТАЦИОННЫХ ИСПЫТАНИЙ.

12. Организационно распорядительная документация разрешительной степени доступа персонала к защищаемым ресурсам АС (обсуждаемым вопросам).
13. Описание технологического процесса обработки информации в АС.
14. Технологические инструкции пользователям АС и администратору безопасности информации.
15. Инструкции по эксплуатации СЗИ.
16. Предписание на эксплуатацию ТСС с приложением протокола спец. исследований ТСС (1 класс)
17. Сертификаты соответствия требованиям по безопасности информации на средства и системы обработки и передачи информации, используемые СЗИ.
18. Данные по уровню подготовки кадров, обеспечивающих ЗИ.
19. Данные о техническом обеспечении средствами контроля эффективности ЗИ и их метрологической поверке.
20. Нормативную и методическую документацию по ЗИ и контролю эффективности защиты.

Операторы ИСПДн

для проведения мероприятий по обеспечению безопасности ПДн (конфиденциальной информации)

при их обработке в ИСПДн 1, 2 классов

и в распределенных информационных системах 3 класса

должны получить лицензию на осуществление деятельности по технической защите конфиденциальной информации в установленном порядке

Заместитель начальника отдела специальных экспертиз
Управления ФСТЭК России
по Приволжскому федеральному округу,
кандидат технических наук

МОКЛЯКОВ
Виталий Александрович