



Код безопасности
ГК «Информзащита»

**Техническая защита персональных
данных в свете вступления в силу
Приказа ФСТЭК №58 от 05.02.2010**

www.securitycode.ru

info@securitycode.ru, +7 (495) 980-2345

Какие средства защиты информации можно применять для защиты персональных данных?

Прежде всего, необходимо определить статус персональных данных с точки зрения законодательства РФ. **Персональные данные относятся к информации ограниченного доступа.**

Персональные данные – это информация ограниченного доступа

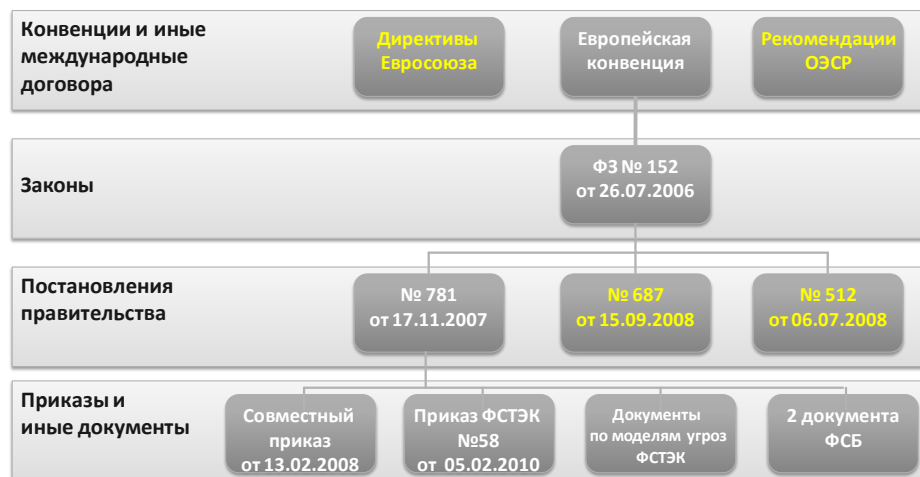
*“Информация, в зависимости от категории доступа к ней, подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (**информация ограниченного доступа**)” (п. 2 ст. 5 закона №149-ФЗ “Об информации, информационных технологиях и о защите информации”).*

*Доступ к персональным данным ограничен в соответствии с законом 152-ФЗ “О персональных данных”: “Операторами и третьими лицами, получающими доступ к персональным данным, **должна обеспечиваться конфиденциальность таких данных...**” (п. 1 ст. 7 закона 152-ФЗ “О персональных данных”) и*

*п. 1 перечня в указе Президента РФ от 23.09.2005 №1111: “Об утверждении сведений конфиденциального характера”: “Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (**персональные данные**), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях”.*

Теперь рассмотрим законодательство РФ и нормативные акты, связанные с защитой персональных данных.

Законодательство в области персональных данных



Согласно Постановлению Правительства №781, для защиты персональных данных должны применяться только СЗИ, в установленном порядке прошедшие процедуру оценки соответствия.

СЗИ должны в установленном порядке проходить оценку соответствия

*“Средства защиты информации, применяемые в информационных системах, **в установленном порядке проходят процедуру оценки соответствия**” (п. 5 Положения об обеспечении безопасности ПДн при их обработке в ИСПДн, утвержденного Постановлением Правительства №781).*

Что это значит? Что это за "оценка соответствия" и как ее можно пройти в "установленном порядке"?

Термины закона "О техническом регулировании"

Закон №184-ФЗ "О ТЕХНИЧЕСКОМ РЕГУЛИРОВАНИИ":

Ст. 2: "оценка соответствия – прямое или косвенное определение соблюдения требований, предъявляемых к объекту;

аккредитация – официальное признание органом по аккредитации компетентности физического или юридического лица **выполнять работы в определенной области оценки соответствия;**

декларирование соответствия – форма подтверждения соответствия продукции требованиям **технических регламентов;**

сертификация – форма осуществляемого органом по сертификации подтверждения соответствия объектов требованиям технических регламентов, положениям стандартов, сводов правил или условиям договоров;

технический регламент – документ, который принят международным договором Российской Федерации, ратифицированным в порядке, установленном законодательством Российской Федерации, или межправительственным соглашением, заключенным в порядке, установленном законодательством Российской Федерации, или федеральным законом, или указом Президента Российской Федерации, или постановлением Правительства Российской Федерации, или нормативным правовым актом федерального органа исполнительной власти по техническому регулированию и устанавливает обязательные для применения и исполнения требования к объектам технического регулирования...;

форма подтверждения соответствия – определенный порядок документального удостоверения соответствия продукции или иных объектов ... положениям стандартов или условиям договоров".

Ст. 7: "Технический регламент должен содержать перечень и (или) описание объектов технического регулирования, требования к этим объектам и правила их идентификации в целях применения технического регламента. Технический регламент должен содержать правила и формы оценки соответствия..."

Оценка соответствия проводится в формах государственного контроля (надзора), аккредитации, испытания, регистрации, **подтверждения соответствия**, приемки и ввода в эксплуатацию объекта, строительство которого закончено, и в иной форме".

Таким образом, оценка – это подтверждение соответствия используемых в ИСПДн средств защиты официально утвержденному и опубликованному техническому регламенту, регулиющему защиту информации в ИСПДн. Оценка проводится только аккредитованными организациями. Форма и схема проведения оценки также должна быть описана в техническом регламенте. В настоящий момент нет такого специального утвержденного технического регламента, а также аккредитованных лабораторий (в области защиты персональных данных). Пока их нет, следует применять действующую нормативную базу, распространяющуюся на персональные данные (ст. 46 закона №184-ФЗ).

Следует отметить, что сертификация также является одной из возможных форм подтверждения соответствия.

Требования ФСТЭК и ФСБ к защите ПДн имеют приоритетный характер

п. 2. ст. 46 закона №184-ФЗ “О техническом регулировании”:

“До дня вступления в силу соответствующих технических регламентов обязательная оценка соответствия, в том числе подтверждение соответствия и государственный контроль (надзор), а также маркирование продукции знаком соответствия осуществляется в соответствии с правилами и процедурами, установленными нормативными правовыми актами Российской Федерации и нормативными документами федеральных органов исполнительной власти, принятыми до дня вступления в силу настоящего Федерального закона”.

Ст. 7: ...Обязательные требования к продукции..., в отношении которых технические регламенты не приняты, действуют до дня вступления в силу соответствующих технических регламентов”.при их обработке в ИСПДн, утвержденного Постановлением Правительства №781).

Дополнительно следует отметить, что в соответствии с п. 5 закона №184-ФЗ, даже если требуемый технический регламент по защите персональных данных и существовал бы, то необходимо было бы выполнить одновременно как требования такого технического регламента, так и требования ФСТЭК и ФСБ в области защиты персональных данных, так как они относятся к информации ограниченного доступа (мы определились с этим в начале статьи).

п. 1 ст. 5 закона №184-ФЗ “О техническом регулировании”:

В отношении ... продукции, используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, обязательными требованиями наряду с требованиями технических регламентов являются требования, установленные государственными заказчиками, федеральными органами исполнительной власти, уполномоченными в области обеспечения безопасности, обороны, внешней разведки, противодействия техническим разведкам и технической защиты информации ... и (или) государственными контрактами (договорами).

Кроме того, следует учесть пункт 18 Положения, утвержденного Постановлением Правительства №781, согласно которому “результаты оценки соответствия СЗИ... оцениваются в ходе экспертизы ФСТЭК/ФСБ”, а такая экспертиза в настоящий момент проводится только в ходе сертификации СЗИ в системе ФСТЭК/ФСБ.

Постановление Правительства РФ №781:

п. 18 Положения: **“Результаты оценки соответствия и (или) тематических исследований средств защиты информации, предназначенных для обеспечения безопасности персональных данных при их обработке в информационных системах, оцениваются в ходе экспертизы, осуществляемой Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий”.**

Сертификация – действующая, легитимная форма подтверждения соответствия

Таким образом, можно сделать вывод о том, что, в настоящий момент, сертификация средств защиты в системе ФСБ/ФСТЭК является легитимной, действующей и юридически оправданной формой подтверждения соответствия средств защиты, применяемых для защиты персональных данных.

Продолжим изучение Постановления №781 дальше.

Постановление Правительства РФ №781:

п. 19 Положения: **“К средствам защиты информации, предназначенным для обеспечения безопасности персональных данных при их обработке в информационных системах, прилагаются правила пользования этими средствами, согласованные с Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий.**

Изменение условий применения средств защиты информации, предусмотренных указанными правилами, согласовывается с этими федеральными органами исполнительной власти в пределах их полномочий”.

п. 20 Положения: **“Средства защиты информации, предназначенные для обеспечения безопасности персональных данных при их обработке в информационных системах, подлежат учету с использованием индексов или условных наименований и регистрационных номеров. Перечень индексов, условных наименований и регистрационных номеров определяется Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий”..**

Надо отметить, что именно в ходе сертификации СЗИ в системе сертификации ФСТЭК и ФСБ выполняются оба указанных требования Постановления №781.

Дополнительные аргументы использования сертифицированных СЗИ

Таким образом, можно сделать общий вывод о том, что **применение сертифицированных СЗИ** для защиты персональных данных – **юридически оправданный и наименее рискованный** путь выполнения требований законодательства в области обеспечения защищенности персональных данных.

Смежные вопросы

1. **Может ли оператор ПДн или интегратор ИБ выполнить самостоятельно декларирование соответствия или сертификацию СЗИ оператора ПДн?**

Декларирование соответствия – нет, так как отсутствует соответствующий технический регламент по защите персональных данных. Сертификацию – да.

2. **Какие виды сертификаций СЗИ допустимы для защиты персональных данных в части обеспечения защищенности?**

По всем видам: ТУ, СВТ, НДВ, ОУД.

3. **Нужен ли сертификат на СЗИ в части отсутствия недекларированных возможностей?**

В п. 7 Приказа ФСТЭК №58 указано на необходимость применения СЗИ, имеющих сертификат НДВ 4, для защиты ИСПДн 1 класса. Для ИСПДн 2 и 3 классов указано такое право оператора ПДн (п. 2.12).

4. **Требуется ли проведение аттестации ИСПДн?**

Требование по проведению аттестации ИСПДн в настоящий момент в действующем законодательстве явно нигде не прописано. Однако ФСТЭК и ФСБ уполномочены проводить мероприятия по контролю/надзору за выполнением требований по технической защите ПДн. Поэтому проект защиты ПДн разумно завершить неким “аудиторским заключением” о достаточности предпринятых мер, позволяющим оператору быть более уверенным, что при проведении проверки его ИСПДн не будет выявлено существенных нарушений. Такой аудит, позволяющий проверять защищенность ИСПДн и ее соответствие требованиям закона, следует проводить ежегодно на договорной основе, так как план проверок формируется раз в год. Преимущество аттестации в том, что аттестат действует три года.

Кроме того, вместо “аудита” оператор может провести аттестацию своей ИСПДн добровольно, с тем чтобы иметь гарантированный документ для проверяющих органов. Легитимность аттестации можно обосновать тем, что в настоящий момент не установлен технический регламент по защите информации ограниченного доступа, что позволяет руководствоваться п. 2. ст. 46 закона №184-ФЗ “О техническом регулировании”:

“До дня вступления в силу соответствующих технических регламентов обязательная оценка соответствия, в том числе подтверждение соответствия и государственный контроль (надзор), а также маркирование продукции знаком соответствия, осуществляется в соответствии с правилами и процедурами, установленными нормативными правовыми актами Российской Федерации и нормативными документами федеральных органов исполнительной власти, принятыми до дня вступления в силу настоящего Федерального закона”.

А процедуры аттестации и сертификации как раз и являются таковыми “нормативными правилами и процедурами”.