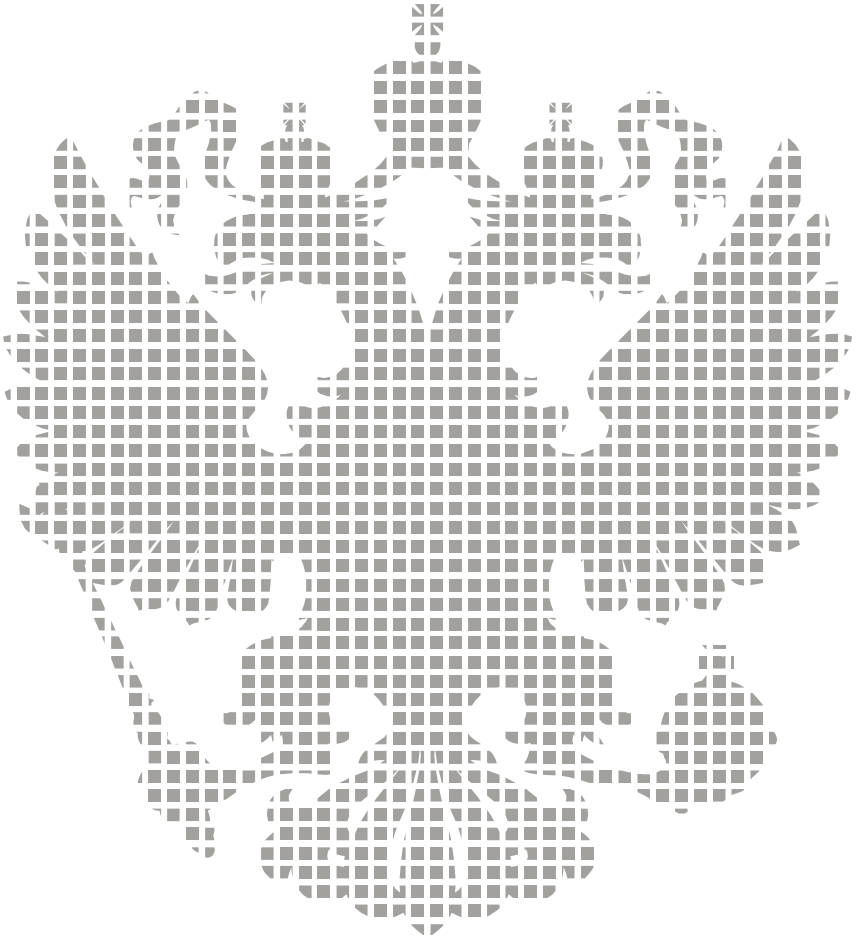
Рекомендации по выполнению требований Федерального закона № 152-ФЗ

«О персональных данных»



Настоящий документ был подготовлен LETA IT-company исключительно в информационных целях. LETA IT-company не несет ответственность за какие-либо убытки или ущерб, возникшие в результате использования сведений, содержащихся в настоящем документе, а также последствия, вызванные неполнотой представленных сведений. Дополнительная информация предоставляется по запросу.

Настоящий документ охраняется законодательством об интеллектуальной собственности и его использование для целей извлечения прибыли не допускается.

Допускается перепечатка, доведение до всеобщего сведения или иное воспроизведение настоящего документа с условием сохранения его целостности и оригинального дизайна, а также с указанием разработчика LETA IT-company.

Любая переработка, за исключением перевода, всего документа или его части допускается лишь с письменного разрешения LETA IT-company.

При цитировании документа ссылка на источник заимствования обязательна.

© LETA IT-company, 2010

Обратите внимание

Приложение-обновление (информационный лист) к сборнику LETA IT-company
«Рекомендации по выполнению требований Федерального закона №152-ФЗ "О персональных данных"»

В связи с принятием 5 февраля 2010 г. ПРИКАЗА ФСТЭК № 58 «*Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных*» и обнародованием РЕШЕНИЯ ФСТЭК, согласно которому **были упразднены** два руководящих документа ФСТЭК:

1) «*Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных*»;
2) «*Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных*» –

просим Вас обратить внимание на важные изменения, затрагивающие проекты по защите персональных данных.

Вышедшие документы значительно изменяют требования к финальным стадиям проектов по защите персональных данных: лицензирование, аттестация и выбор сертифицированных средств защиты информации (СЗИ).

Согласно этим документам:

- организации, проводящие работы по защите персональных данных для собственных нужд и не оказывающие подобные услуги третьим лицам, могут **не получать лицензию ФСТЭК России** на деятельность по технической защите конфиденциальной информации. В случае, если для проведения работ по защите персональных данных организация привлекает стороннюю компанию, то привлекаемый исполнитель должен обладать упомянутой лицензией;
- **аттестация** построенной системы защиты персональных данных **не является обязательной** (до выхода соответствующего положения ФСТЭК России);
- использование СЗИ, прошедших оценку соответствия на отсутствие недекларируемых возможностей (НДВ), является **обязательным только для информационных систем персональных данных (ИСПДн) класса К1**. Для остальных классов ИСПДн использование СЗИ, прошедших данный вид оценки соответствия, является **необязательным** и остается **на усмотрение оператора**. Таким образом, в настоящее время оператор (эксплуатирующий ИСПДн ниже класса К1) для построения системы защиты персональных данных может использовать любые СЗИ, прошедшие сертификацию ФСТЭК по ТУ, что в значительной мере расширяет возможность выбора СЗИ. Тем не менее при выборе СЗИ необходимо руководствоваться требованиями, описанными в «Приложении 1 к положению о методах и способах защиты информации в информационных системах персональных данных».

В связи с вышеизложенным сборник «Рекомендации по выполнению требований Федерального закона №152-ФЗ "О персональных данных"» остается актуальным, приобретая более высокую значимость в связи с продлением дедлайна по 152-ФЗ до 01.01.2011.

Оглавление

Приветственное слово Генерального директора LETA IT-company 4

Введение 5

1. Список терминов 8

2. Список сокращений 10

3. Общий порядок действий оператора по выполнению требований федерального закона № 152-ФЗ «О персональных данных» 11

   Шаг 1. Определить структурное подразделение или должностное лицо, ответственное за обеспечение безопасности ПДн 16

   Шаг 2. Определить состав обрабатываемых ПДн, цели и условия обработки. Определить срок хранения ПДн 23

   Шаг 3. Получить согласие субъекта на обработку его ПДн, в том числе в письменной форме 27

   Шаг 4. Определить порядок реагирования на запросы со стороны субъектов персональных данных 32

   Шаг 5. Определить необходимость уведомления уполномоченного органа по защите ПДн о начале обработки ПДн. Если необходимость есть, то составить и отправить уведомление 37

   Шаг 6. Выделить и классифицировать ИСПДн 42

   Шаг 7. Разработать модель угроз для ИСПДн 49

   Шаг 8. Спроектировать и реализовать систему защиты персональных данных 54

   Шаг 9. Провести аттестацию ИСПДн по требованиям безопасности или продекларировать соответствие 61

   Шаг 10. Определить перечень мер по защите ПДн, обрабатываемых без использования средств автоматизации 65

   Шаг 11. Обеспечить постоянный контроль защищённости ПДн 69

4. Заключение 73

5. Список нормативно-правовых документов 74

6. Полезные ссылки 76

7. О LETA IT-company 78

Уважаемые коллеги!

Для большинства из нас вопрос выполнения требований федерального закона №152-ФЗ «О персональных данных» был одним из самых актуальных вопросов в течение 2009 года.

Многие ИТ и ИБ руководители потратили немало сил, пытаясь разобраться во всех тонкостях и противоречиях законодательства в данной сфере, чтобы выработать оптимальный путь выполнения требований государства. Однако самостоятельно решить данную задачу смогли единицы, а выполнять требования закона должны все.

При этом подавляющее большинство выступлений экспертов, проблемных статей, семинаров и конференций по теме защиты персональных данных давали лишь общее введение в законодательные вопросы и очень активно обращали внимание аудитории на огромное количество противоречий в различных руководящих документах. А наиболее насущные вопросы о том, как фактически переложить достаточно объёмные и сложные требования закона на реальную организацию со сложившейся практикой работы, и с чего начать, практически всегда оставались за кадром.

Без лишней скромности скажу, что эксперты LETA были одними из немногих, кто на протяжении этого года пытался доносить до рынка конкретные рекомендации и делиться реальным практическим опытом, полученным в рамках наших консалтинговых проектов. За год мы организовали и провели 8 семинаров и мастер-классов, приняли участие в десятках конференций и форумов, написали более пятнадцати статей по данной теме.

Однако, оценив всю эту работу, мы отчетливо поняли, что этих усилий недостаточно для полноценного донесения необходимых знаний до всех, кому они нужны и важны. Да и форматы выступлений на конференциях или статей в прессе не позволяют раскрыть тему с необходимым уровнем детализации.

В связи с этим руководством LETA было принято решение о реализации проекта по созданию самоучителя по выполнению требований закона «О персональных данных». Результатом данной работы и стал документ, который в настоящий момент находится перед Вами.

Я искренне надеюсь, что результаты наших многодневных трудов принесут Вам пользу и помогут создать у себя в организации систему защиты персональных данных, не только соответствующую формальным требованиям закона, но и реально повышающую уровень защиты информации.

Андрей Юрьевич Конусов,
Генеральный директор LETA IT-company

Введение

Защита персональных данных является одной из важнейших задач системы обеспечения информационной безопасности в организации любого масштаба и любой организационно-правовой формы. Нарушение режима конфиденциальности имеющихся в организации данных клиентов, сотрудников, обслуживаемых граждан является само по себе серьёзнейшим инцидентом информационной безопасности, создающим многочисленные риски.

Это и финансовые риски, связанные с необходимостью затрат на срочные меры реакции на инцидент (проведение расследования, организация «аварийных» PR-мероприятий), и имиджевые риски, и чисто коммерческие, связанные с утратой лояльности клиентов и их оттоком. Достаточно того резонанса, который обычно вызывают ставшие достоянием гласности случаи утечки массивов персональных данных. Например, базы данных, предлагаемые на «черном рынке».

Но если еще совсем недавно каждая организация, обрабатывающая персональные данные, заботилась об их защите исходя из собственных представлений, зафиксированных во внутренних политиках информационной безопасности, то теперь ситуация изменилась. Правила в этой игре отныне устанавливает государство. Каждая организация обязана обеспечить некоторый необходимый уровень защиты персональных данных, которыми оперируют её сотрудники. Но, как это зачастую происходит, введение жёсткого государственного контроля, независимо от области регулирования, связано с появлением неопределённости для лиц, попадающих в поле контроля. Особенно, если речь идёт о регулировании отношений, сложившихся годами, зачастую пронизывающих все основные информационные процессы в организациях.

Всё работает, зачем нам что-то менять в обработке персональных данных? Именно этот вопрос был естественной реакцией многих руководителей на информацию о появлении закона «О персональных данных». Увы, достаточно было услышать их ответы на два-три вопроса, касающиеся организации защиты персональных данных, чтобы понять: существующая система защиты не соответствует множеству требований, установленных законодательством о защите персональных данных. Но, в силу сложившихся веками традиций отношения к законодательным нововведениям, с неизбежностью возникал следующий вопрос…

Может, меня это всё не коснется? Ведь закон затрагивает практически любого хозяйствующего субъекта, государственную или муниципальную организацию – очевидно, что регулирующему органу не хватит имеющихся ресурсов на объективную проверку даже 1% операторов персональных данных. Да и что с того: одним проверяющим больше, одним меньше… В целом оптимальной тактикой многим представлялось отсутствие какой-то деятельности. Стоит ли открывать проект, если законодательство может ещё не раз поменяться? Нужно ли подавать уведомление об обработке персональных данных, если это с неизбежностью приведёт к попаданию в фокус контролирующего органа власти? Именно в таком состоянии застал нас 2009 год. Но надежда на то, что «авось пронесет», растаяла к концу года, когда всему сообществу стало ясно, что закон начинает работать, а сами требования к защите персональных данных, безусловно, важны и требуют самого серьёзного к себе отношения. Регистрация десятков тысяч организаций в качестве

операторов персональных данных, зарождение правоприменительной практики по требованиям закона, появления списка плановых проверок на сайте Роскомнадзора, выход массива руководящих документов ФСБ России и ФСТЭК России – всё это, судя по всему, окончательно убедило бизнес и ИТ-руководителей всех уровней, что тема требует самого внимательного отношения.

Более чем серьезным является отношение к данной тематике и Государственной Думы Российской Федерации, которое более чем ясно было выражено в докладах в рамках Парламентских слушаний. Безусловно, закон и подзаконные акты по данной тематике всё ещё несовершенны и должны быть доработаны, и ни у кого не возникает сомнений в необходимости существования нормально работающего законодательства о защите персональных данных. Таким образом, с пониманием того, что исполнение норм закона необходимо обеспечивать, мы подошли к другому вечному вопросу.

Что собственно делать? Как строить работу по проекту построения системы защиты персональных данных? И на этот вопрос ответить непросто по ряду причин, и вот лишь некоторые из них:

1. Федеральный закон или какой-либо иной нормативный акт не дают единого порядка проведения работ по приведению системы защиты персональных данных в соответствие с законом.
2. Закон действительно содержит немало противоречий нормам действующего законодательства и несёт в себе ряд не вполне ясных формулировок.
3. Организовать работы по построению системы защиты персональных данных невозможно без знания действующих руководящих документов (РД) в области защиты конфиденциальной информации.
4. Идеология большинства руководящих документов не вполне соответствует современным реалиям. А если сказать точнее, существующие системы обеспечения ИБ в коммерческих организациях в массе своей построены без учёта требований этих РД.
5. Многие аспекты построения систем защиты персональных данных, такие так оценка соответствия объекта информатизации, практически не отрегулированы.

Тем не менее, в 2008-2009 годах сложилась практика ведения проектов по построению систем защиты персональных данных, которая позволяет сформулировать общую канву ведения проектов и разрешить большинство сложных актуальных вопросов.

Обобщив практику ведения ряда проектов в области защиты персональных данных, группа экспертов компании LETA попыталась свести воедино описание всех основных этапов такого проекта, представленного как последовательность отдельных шагов.

Для каждого шага приводится:

- цель шага, его назначение в общей канве проекта;
- основание и описание состава основных работ на данном шаге;
- основной результат, который достигается по результатам шага;
- некоторые важные особенности исполнения шага, на которые непременно следует обратить внимание;
- список основных нормативно-правовых актов, относящихся к данному шагу.

Таким образом, главная цель этого материала – донести общую картину реализации проекта по построению системы защиты персональных данных, без понимания которой практически невозможно сделать первый шаг в сторону исполнения требований закона и попробовать самостоятельно реализовать его требования. Имея ясное представление о назначении и содержании отдельных шагов в рамках проекта, специалистам будет существенно проще донести потребности компании в области защиты персональных данных до руководства и заручиться его поддержкой, реалистично оценить сроки и стоимость реализации проекта, выделить ряд аспектов, по которым придется принимать принципиальное решение, достойно подготовиться к встрече с проверяющими органами.

И хотя, на первый взгляд, работа эта может показаться огромной, как говорится, дорогу осилит идущий. И настоящий материал, безусловно, должен помочь в этом деле. Проект построения системы защиты персональных данных вполне реализуем, хотя и предполагает вовлечение в него существенных сил и ресурсов.

1. Список терминов

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи

Информационная система персональных данных – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределённое программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Модель нарушителя – предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности.

Модель угроз – документ, содержащий перечень возможных угроз безопасности персональных данных при их обработке в информационных системах персональных данных и характеризующий наступление различных видов последствий в результате несанкционированного или случайного доступа и реализации угроз безопасности персональных данных.

Недекларированные возможности – функциональные возможности средств вычислительной техники и (или) программного обеспечения, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам.

Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

Персональные данные – любая информация, относящаяся к определённому или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты её функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Система защиты персональных данных – совокупность организационные мер и технических средств защиты информации, а также используемых в информационной системе информационных технологий, в рамках которых реализуются организационные и технических мероприятия, обеспечивающие безопасность 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 (защищённость от уничтожения, изменения, блокирования, а также иных несанкционированных действий).

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект персональных данных – физическое лицо, к которому относятся определённые персональные данные либо которое может быть определено на основании определённых персональных данных.

Типовые информационные системы – информационные системы, в которых требуется обеспечение только конфиденциальности персональных данных.

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Частная модель угроз – модель угроз применительно к конкретным условиям функционирования ИСПДн.

2. Список сокращений

АСЗИ – автоматизированная система в защищённом исполнении.

ВТСС – вспомогательные технические средства и системы.

ИБ – информационная безопасность.

ИСПДн – информационная система персональных данных.

КЗ – контролируемая зона.

МЭ – межсетевой экран.

НДВ – недекларированные возможности.

НМД – нормативно-методический документ.

НСД – несанкционированный доступ.

ПДн – персональные данные.

ПЭМИН – побочные электромагнитные излучения и наводки.

РД – руководящий документ.

СЗИ – средство защиты информации.

СЗПДн – система защиты персональных данных.

СКЗИ – средство криптографической защиты информации.

СУИБ – система управления информационной безопасностью.

ТЗ – техническое задание.

ТЗКИ – техническая защита конфиденциальной информации.

ЧТЗ – частное техническое задание.

3. Общий порядок действий оператора по выполнению требований федерального закона № 152-ФЗ «О персональных данных»

3.1. Общие требования

Вне зависимости от того, привлекает ли организация для проведения работ, связанных с выполнением требований федерального закона № 152-ФЗ «О персональных данных», специализированную стороннюю организацию или строит систему защиты самостоятельно, она должна решить следующие основные задачи.

Определение области внедрения. Должны быть определены объекты (территории, офисы, филиалы, представительства), структурные подразделения, автоматизированные системы и процессы, в границах которых будут осуществляться мероприятия по реализации требований закона к порядку обработки персональных данных.

Назначение ответственных. Должно быть определено структурное подразделение или должностное лицо, ответственное за обеспечение безопасности ПДн.

Разработка и утверждение перечня персональных данных. Необходимо определить состав обрабатываемых ПДн, цели и условия обработки, сроки хранения ПДн различных категорий. Перечень обрабатываемых в ИСПДн персональных данных должен быть утверждён приказом руководителя.

Установление необходимого уровня правоотношений между оператором и субъектом персональных данных. Согласие субъекта на обработку его ПДн должно быть при необходимости получено, в том числе и в письменной форме. В целях обеспечения максимальной юридической чистоты в вопросах соблюдения прав субъектов персональных данных и во избежание инцидентов, связанных с нарушением этих прав, порядок реагирования на запросы со стороны субъектов персональных данных, внесения изменений в ПДн, а также условия прекращения обработки ПДн должны быть также определены документально в соответствующих приказах, инструкциях и процедурах, определяющих в том числе степень участия должностных лиц в обработке ПДн и характер их взаимодействия между собой.

Выделение и классификация ИСПДн. ИСПДн, подлежащие защите, должны быть однозначно идентифицированы как совокупности конкретных технических средств, размещенных внутри конкретных контролируемых зон и предназначенных для обработки конкретных категорий ПДн с конкретными целями. Должна быть проведена их классификация. На каждую ИСПДн должен быть оформлен отдельный Акт классификации.

Разработка модели угроз и требований к системе защиты. Разработка модели угроз входит в состав мероприятий по обеспечению безопасности ПДн при их обработке в информационных системах, предусмотрена методическими документами ФСТЭК России и ФСБ России в качестве обязательной меры для специальных ИСПДн. Модель угроз разрабатывается в соответствии с методическими документами ФСТЭК России и ФСБ России. При этом в зависимости от характеристик конкретной ИСПДн применяются документы либо одного, либо обоих ведомств. Требования по обеспечению безопасности ПДн разрабатываются на основе модели угроз с учётом установленного класса ИСПДн и включаются в техническое (частное техническое) задание на разработку СЗПДн.

Проектирование и создание ИСПДн (СЗПДн). В каждой информационной системе, предназначенной для обработки ПДн, должна быть спроектирована и создана система защиты персональных данных, соответствующая требованиям руководящих и нормативно-методических документов ФСТЭК России и ФСБ России по защите информации. Порядок проектирования определяется рядом государственных стандартов и руководящих документов ФСТЭК России.

Подтверждение соответствия ИСПДн (СЗПДн) требованиям к безопасности ПДн. Предусматриваются различные способы оценки соответствия в зависимости от характеристик объекта оценки (техническое средство, программное обеспечение, средство защиты информации, система в целом) и целей проведения оценки. В соответствующих разделах настоящего документа рассматриваются такие виды оценки, как аттестация и декларирование соответствия.

Обеспечение контроля над обеспечением уровня защищённости ПДн. После проведения оценки соответствия и ввода в действие ИСПДн с внедрённой в её состав системой защиты персональных данных должно быть обеспечено выполнение всех требований по защите при её эксплуатации. С этой целью в организации организовывается и проводится периодический контроль эффективности применяемых мер защиты, в том числе с применением специальных сертифицированных средств контроля.

Направление уведомления о начале обработки персональных данных. Выполнив все установленные требования к СЗПДн в своей информационной системе, оператор получает право начать обработку персональных данных. До начала обработки он обязан уведомить об этом уполномоченный орган по защите прав субъектов персональных данных (Роскомнадзор). Порядок уведомления, содержание представляемых материалов, а также случаи, когда разрешается осуществлять обработку ПДн без уведомления уполномоченного органа, определены в законе (статья 22).

Получение лицензий ФСТЭК России и ФСБ России. В ряде предусмотренных федеральным законодательством случаев организация, осуществляющая деятельность, связанную с использованием сертифицированных средств криптографической защиты информации, либо деятельность в области технической защиты конфиденциальной информации должна получить соответствующие лицензии. Так, ФСБ России на основании Постановления Правительства РФ от 29 декабря 2007 г. № 957 требует от всех организаций, эксплуатирующих средства криптографической защиты информации (СКЗИ), получать лицензии на техническое обслуживание СКЗИ, а также другие лицензии ФСБ России. ФСТЭК России в своих методических документах по защите ПДн указывает на обязанность операторов, эксплуатирующих ИСПДн 1 и 2 классов и распределённые ИСПДн 3 класса, получать лицензии на деятельность по технической защите конфиденциальной информации.

Выполнение прочих требований закона. Федеральным законом № 152-ФЗ «О персональных данных» и подзаконными актами установлен ряд других норм и требований, которые могут иметь отношение не ко всем операторам и которые должны исполняться теми из них, для кого это является производственной необходимостью. Это и обработка биометрических персональных данных, и вопросы трансграничной передачи персональных данных, и учёт особенностей обработки персональных данных без

использования средств автоматизации. При наличии таких оснований требуется выработка специальных мер, разработка процедур и издание внутренних организационно-распорядительных документов, регулирующих данные процессы.

3.2. Требования к СЗПДн

Задача проектирования и создания СЗПДн является одной из самых сложных, интеллектуально- и трудоёмких задач, связанных с исполнением требований ФЗ «О персональных данных», требующих наибольшего вложения финансовых средств. Данный вопрос требует отдельного, более детального освещения, и в настоящем документе ему уделено особое внимание.

Проектирование и создание СЗПДн должно осуществляться в соответствии с руководящими и нормативно-методическим документами регуляторов – ФСТЭК России и ФСБ России. И прежде всего – ФСТЭК России, поскольку общие вопросы построения систем защиты регулируются именно этим органом. Именно научно-исследовательскими организациями ФСТЭК России разработаны соответствующие государственные стандарты для автоматизированных систем в защищённом исполнении. Методические документы ФСБ России не содержат рекомендаций по порядку проектирования систем защиты и предназначены для применения лишь в случае использования СКЗИ для защиты ПДн.

На стадии проектирования и создания СЗПДн проводится комплекс проектных и конструкторских работ, предусмотренный государственными стандартами, руководящими и методическими документами в области защиты информации. При этом в полном объёме учитываются как организационные, так и технические аспекты. Организационные аспекты заключаются в формировании и реализации совокупности согласованных по цели, задачам, месту и времени организационных и технических мероприятий, направленных на обеспечение безопасности ПДн при их обработке в ИСПДн, а также минимизацию ущерба субъекту персональных данных от возможной реализации угроз безопасности ПДн. Технические аспекты связаны с наличием чётко документированных требований по закрытию технических каналов утечки ПДн, а также по защите ПДн от несанкционированного доступа при их обработке в информационных системах. Применяемые в этих целях средства защиты информации должны быть сертифицированы.

При разработке СЗПДн следует чётко представлять себе методологии, разработанные в ФСТЭК России для защиты конфиденциальной информации, и непосредственно руководствоваться следующими руководящими и методическими документами:

- ГОСТ Р 51583-2000 «Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Основные положения» (для служебного пользования);
- ГОСТ Р 51624-2000 «Защита информации. Автоматизированные системы в защищённом исполнении. Основные положения» (для служебного пользования);
- Руководящий документ «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)». Утвержден приказом Гостехкомиссии России от 30 августа 2002 г. № 282 (для служебного пользования);
- Методический документ «Основные мероприятия по организации и техническому обеспечению безопасности ПДн, обрабатываемых в информационных системах

персональных данных», ФСТЭК России, 15 февраля 2008 г. (пометка «для служебного пользования» снята решением ФСТЭК России от 16 ноября 2009 г.);
- Методический документ «Рекомендации по обеспечению безопасности ПДн при их обработке в информационных системах персональных данных», ФСТЭК России, 15 февраля 2008 г. (пометка «для служебного пользования» снята решением ФСТЭК России от 16 ноября 2009 г.).

3.3. Стадии создания СЗПДн

Согласно СТР-К, РД «Основные мероприятия…» и ГОСТ Р 51583-2000, создание СЗПДн должно включать следующие стадии и этапы:

- ***предпроектная стадия,*** включающая предпроектное обследование ИСПДн, разработку технического (частного технического) задания на её создание;
- ***стадия проектирования и реализации ИСПДн,*** включающая разработку СЗПДн в составе ИСПДн;
- ***стадия ввода в действие СЗПДн,*** включающая опытную эксплуатацию и приёмо-сдаточные испытания, а также оценку соответствия ИСПДн требованиям безопасности информации.

3.3.1. Предпроектная стадия

В ходе предпроектного обследования ИСПДн:

- определяется перечень ПДн, обрабатываемых в ИСПДн, и в них выделяется совокупность ПДн, подлежащих защите;
- определяются условия размещения технических средств ИСПДн относительно контролируемой зоны и доступа к ним;
- определяются конфигурация и топология ИСПДн, физические, функциональные и технологические связи как внутри ИСПДн, так и с другими системами;
- определяются технические средства и системы, составляющие ИСПДн, используемые общесистемные и прикладные программные средства;
- определяются режимы обработки ПДн в ИСПДн в целом и в отдельных компонентах;
- определяется класс ИСПДн;
- уточняется степень участия должностных лиц в обработке ПДн, характер их взаимодействия между собой;
- определяются (уточняются) угрозы безопасности ПДн применительно к конкретным условиям функционирования ИСПДн, разрабатывается модель угроз.

По результатам предпроектного обследования разрабатывается техническое (частное техническое) задание на разработку СЗПДн, в которое включаются конкретные требования по обеспечению безопасности ПДн при их обработке в ИСПДн.

3.3.2. Стадия проектирования и реализации ИСПДн

Стадия проектирования и создания ИСПДн включает разработку СЗПДн в составе ИСПДн. На данной стадии в соответствии с требованиями ТЗ (ЧТЗ) на разработку СЗПДн:

- разрабатывается задание на проведение работ, и выполняются работы в соответствии с проектной документацией;

- разрабатываются мероприятия по защите информации в соответствии с предъявляемыми требованиями;
- проводится обоснование состава и закупка технических средств ИСПДн и сертифицированных средств защиты информации и их установка;
- разработка эксплуатационной и организационно-распорядительной документации на ИСПДн по обеспечению режима информационной безопасности при обработке ПДн и разрешительной системы доступа пользователей к обрабатываемой в ИСПДн информации;
- выполняются другие мероприятия, характерные для конкретных ИСПДн и направлений обеспечения безопасности ПДн.

3.3.3. Стадия ввода в действие СЗПДн

На стадии ввода в действие СЗПДн осуществляются:

- опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИСПДн;
- приемо-сдаточные испытания СЗПДн по результатам опытной эксплуатации;
- оценка соответствия ИСПДн требованиям по безопасности ПДн.

Решение вышеописанных основных типовых задач, стоящих перед операторами при реализации требований закона № 152-ФЗ «О персональных данных», может быть представлено в виде следующих одиннадцати шагов:

1. Определить структурное подразделение или должностное лицо, ответственное за обеспечение безопасности ПДн.
2. Определить состав обрабатываемых ПДн, цели и условия обработки. Определить срок хранения ПДн.
3. Получить согласие субъекта на обработку его ПДн, в том числе в письменной форме.
4. Определить порядок реагирования на запросы со стороны субъектов персональных данных.
5. Определить необходимость уведомления уполномоченного органа по защите ПДн о начале обработки ПДн. Если необходимость есть, то составить и отправить уведомление.
6. Выделить и классифицировать ИСПДн.
7. Разработать модель угроз для ИСПДн.
8. Спроектировать и реализовать СЗПДн.
9. Провести аттестацию ИСПДн по требованиям безопасности или продекларировать соответствие.
10. Определить перечень мер по защите ПДн, обрабатываемых без использования средств автоматизации.
11. Выполнять постоянный контроль над обеспечением уровня защищённости ПДн.

Создание детализированного описания данных шагов и стало основной задачей данной брошюры.

Шаг 1.
Определить структурное подразделение или должностное лицо, ответственное за обеспечение безопасности ПДн

Введение

Распределение ролей и ответственности персонала за обеспечение требований по ИБ в организации всегда рассматривалось как важнейшее требование и в международной практике, и в отечественном правовом поле.

Так, еще в Положении о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от её утечки по техническим каналам, введённом в действие постановлением Совета Министров – Правительства РФ от 15 сентября 1993 года № 912-51 (п. 18), было определено, что организация работ по защите информации на предприятиях осуществляется их руководителями, и в зависимости от объёма работ по защите информации руководителем предприятия создаётся структурное подразделение по защите информации либо назначаются штатные специалисты по этим вопросам.

А определение ответственности и обязанностей в области ИБ названо в международном стандарте BS ISO/IEC 27001:2005 и соответствующем ему национальном стандарте РФ ГОСТ Р ИСО/МЭК 27001-2006 обязательной для применения мерой информационной безопасности и одним из доказательств исполнения обязанностей руководства по разработке и поддержанию системы управления информационной безопасностью.

Если структурное подразделение либо штатный специалист по защите информации в организации не назначены, ответственность за выполнение требований к безопасности ПДн, установленных законодательством и нормативно-правовыми актами Российской Федерации, целиком ложится на руководителя предприятия-оператора.

Цели проведения работ

Целями этапа являются:

- определение должностных лиц и структурных подразделений, ответственных за информационную безопасность и соблюдение требований нормативно-правовых актов Российской Федерации, регламентирующих порядок защиты ПДн;
- разработка и утверждение внутренних документов (положений, инструкций и т.п.), регламентирующих деятельность структурных подразделений, отвечающих за ИБ;
- разработка и утверждение документов, закрепляющих функциональные обязанности и права должностных лиц и структурных подразделений, отвечающих за информационную безопасность.

Основание проведения работ

Согласно пункту 3.2 методического документа ФСТЭК России «Основные мероприятия…», для разработки и осуществления мероприятий по организации и обеспечению безопасности ПДн при их обработке в ИСПДн оператором или уполномоченным им лицом должно назначаться структурное подразделение или должностное лицо (работник), ответственное за обеспечение безопасности ПДн.

А согласно пункту 3.10 того же документа, на стадии проектирования и создания ИСПДн должны быть определены подразделения и назначены должностные лица, ответственные за эксплуатацию средств защиты информации, с их обучением по направлению обеспечения безопасности ПДн.

Эта норма полностью соответствует положениям ГОСТ Р 51583-2000 «Порядок создания автоматизированных систем в защищённом исполнении», согласно которому общее руководство работами по защите информации при создании автоматизированной системы в защищённом исполнении (АСЗИ) в целом осуществляет главный конструктор АСЗИ или его заместители, а при создании компонентов АСЗИ — главные конструктора этих компонентов или их заместители. При этом методическое руководство работами по защите информации в системе осуществляют подразделения организаций (штатные специалисты) по ЗИ, участвующие в создании АСЗИ.

Согласно методическому документу ФСБ России «Типовые требования…» (п.2.6), обеспечение функционирования и безопасности криптосредств возлагается на ответственного пользователя криптосредств, имеющего необходимый уровень квалификации, назначаемого приказом оператора (далее – ответственный пользователь криптосредств).

Допускается возложение функций ответственного пользователя криптосредств на:

- одного из пользователей криптосредств;
- на структурное подразделение или должностное лицо (работника), ответственных за обеспечение безопасности ПДн, назначаемых оператором;
- на специальное структурное подразделение по защите государственной тайны, использующее для этого шифровальные средства.

Выполняемые работы

В соответствии с требованиями Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ст. 4), обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

- предотвращение несанкционированного доступа к информации и (или) передачи её лицам, не имеющим права на доступ к информации;
- своевременное обнаружение фактов несанкционированного доступа к информации;
- предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

- недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
- возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
- постоянный контроль за обеспечением уровня защищённости информации.

Из данной статьи 4 федерального закона следует необходимость выполнения следующих условий:

- обработка защищаемой информации регламентирована, проводится регулярный контроль соблюдения установленного порядка обработки;
- защита информации организована, проводится постоянный контроль и оценка эффективности данной защиты;
- физическая защита элементов инфраструктуры, участвующих в обработке защищаемой информации, организована, проводится регулярный контроль эффективности защиты.

Фактически в каждой организации-операторе в той или иной степени все эти процессы были регламентированы еще до принятия закона № 152-ФЗ. С введением новых требований появилась потребность привести процессы в соответствие с вновь установленными нормами. Важным является то, что многие требования по обеспечению безопасности ПДн в точности соответствуют или вытекают из требований по организации и обеспечению безопасности информации с ограниченным доступом.

Для того, чтобы процесс актуализации системы защиты ПДн, а также поддержания её в состоянии, соответствующем требованиям нормативно-правовых актов Российской Федерации, был управляем, на этапе принятия решения о формировании системы управления информационной безопасностью организации-оператора необходимо определить коллегиальный орган или должностное лицо, которое будет координировать деятельность по созданию системы защиты. Это ответственное лицо должно регулярно оценивать достаточность и эффективность СЗПДн и нести дисциплинарную, административную, уголовную и другую ответственность, предусмотренную за невыполнение требований закона № 152-ФЗ. В случае небольшого круга ответственности функции данного должностного лица могут быть возложены на нештатного сотрудника, ответственного за ИБ.

Назначение структурных подразделений и ответственных лиц осуществляется исключительно приказами руководителя организации-оператора.

В обеспечение деятельности назначенных структурных подразделений и ответственных должностных лиц в организации должны быть разработаны Положения о данных подразделениях и должностных лицах. Обязательным условием является включение в данные Положения разделов, определяющих не только функции и обязанности, но и права, и ответственность за исполнение данных функций и обязанностей.

Для каждого сотрудника подразделения по ИБ должны быть разработаны индивидуальные, соответствующие его зоне ответственности и обязанностям должностные инструкции.

При достаточно сложной производственной структуре организации-оператора должны быть разработаны регламенты и процедуры взаимодействия подразделений и сотрудников по ИБ с другими структурными подразделениями оператора и распределены роли и ответственность подразделений, не отвечающих за исполнение требований по ИБ, но вовлеченных в деятельность, связанную с использованием информации конфиденциального характера (ПДн). Указанные регламенты и процедуры могут быть исполнены в виде текстовых и графических (схем взаимодействия) материалов и изданы как в качестве отдельных документов, так и в виде разделов документов системы управления информационной безопасностью более высокого уровня. Таким документом может быть, например, Руководство, разрабатываемое в соответствии с Типовыми требованиями к содержанию и порядку разработки Руководства по защите информации от технических разведок и от её утечки по техническим каналам, одобренными решением Гостехкомиссии России от 03 октября 1995 г. № 42.

Результат

Результатом первого шага является документированное закрепление ролей, полномочий, прав, обязанностей и ответственности должностных лиц и подразделений организации-оператора в процессах, имеющих отношение к обеспечению ИБ организации-оператора.

Должны быть разработаны соответствующие внутренние нормативно-методические и организационно-распорядительных документы:

- для организации-оператора – Руководство по защите информации от технических разведок и от её утечки по техническим каналам, регламенты и процедуры;
- для подразделения – Положение о структурном (производственном) подразделении;
- для должностного лица – его должностная инструкция.

Указанные документы должны быть утверждены (введены в действие) приказом генерального директора и быть доведены до лиц, вовлеченных в деятельность, связанную с необходимостью выполнять требования к безопасности информации, под роспись. Обязанность выполнения указанных требований должна быть зафиксирована в трудовых договорах с сотрудниками организации-оператора.

При необходимости в результате первого шага должны быть также скорректированы должностные инструкции и трудовые договора работников организации-оператора, не входящих непосредственно в подразделение, осуществляющее функции по обеспечению безопасности информации, и не назначенных ответственными сотрудниками в этой области, но причастных к деятельности, связанной с необходимостью выполнять требования к безопасности конфиденциальной информации (ПДн).

Таким образом, материальным результатом работ на данном шаге является пакет приказов, руководств, положений, регламентов, процедур, трудовых договоров, должностных инструкций и прочих документов, регламентирующих все стороны деятельности подразделений и сотрудников по ИБ, включая их функции, обязанности, права и ответственность.

Ограничения / на что стоит обратить внимание

В течение десятков лет развития Государственной системы защиты информации сложились типовые структуры управления информационной безопасностью предприятий. Традиционное представление о них нашло отражение в соответствующих разделах руководящего документа Гостехкомиссии России «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)». И распределение ролей подразделений и должностных лиц предприятий, их ответственности за обеспечение ИБ постоянно находилось в сфере внимания регулирующих органов, в том числе при проведении проверок выполнения установленных норм и требований по технической защите конфиденциальной информации.

С учётом того, что методический документ ФСТЭК России «Рекомендации по обеспечению безопасности ПДн при их обработке в информационных системах персональных данных» ориентирует операторов на использование традиционных подходов к технической защите информации в автоматизированных системах, необходимо в этой работе следовать также рекомендациям СТР-К.

Так, согласно пункту 3.2 интернет-версии данного документа, организация работ по защите информации возлагается на руководителей учреждений и предприятий, руководителей подразделений, осуществляющих разработку проектов объектов информатизации и их эксплуатацию, а методическое руководство и контроль за эффективностью предусмотренных мер защиты информации – на руководителей подразделений по защите информации (служб безопасности) учреждения (предприятия).

В отсутствие в организации-операторе структурного подразделения по защите информации ответственность за организацию, равно как и осуществление работ по обеспечению ИБ могут быть возложены на любого сотрудника организации, наиболее подготовленного в области технической защиты конфиденциальной информации (ТЗКИ) или близкой к ней. Но в некоторых случаях – например, при получении лицензий на определённые виды деятельности, – требования могут быть намного жёстче.

Так, в соответствии с «Положением о лицензировании деятельности по технической защите конфиденциальной информации», утверждённым Постановлением Правительства Российской Федерации от 15 августа 2006 г. № 504, наличие в штате соискателя лицензии (лицензиата) специалистов, имеющих высшее профессиональное образование в области технической защиты информации либо высшее или среднее профессиональное (техническое) образование и прошедших переподготовку или повышение квалификации по вопросам ТЗКИ является одним из основных лицензионных требований и условий при осуществлении деятельности по технической защите конфиденциальной информации.

Аналогичные ограничения со стороны ФСБ России более строги. Для отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами, соответствующими Положениями, утверждёнными постановлением правительства РФ от 29 декабря 2007 г. № 957, предусмотрено наличие у лица, уполномоченного руководить работами по лицензируемой деятельности, высшего профессионального образования и

(или) профессиональной подготовки в области ИБ, а также стажа работы в этой области не менее 5 лет.

Следует помнить, что обработка ПДн ведется не только в информационных системах. ПДн могут существовать не только в электронном, но и в бумажном виде, и храниться на других (магнитных, оптических и т.д.) носителях, для которых установлен особый порядок хранения, учёта и обращения. Этот порядок регламентирован в настоящее время лишь Положением о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, введённым постановлением Правительства РФ от 3 ноября 1994 г. № 1233. Согласно данному Положению, приём и учёт (регистрация) документов, содержащих служебную информацию ограниченного распространения, осуществляются, как правило, структурными подразделениями, которым поручен приём и учёт несекретной документации. Данное Положение полностью применимо при формировании системы защиты персональных данных, обрабатываемых без использования средств автоматизации, которая строится с учётом постановления Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации». И поэтому в организации могут быть разделены роли и ответственность сотрудников, отвечающих за техническую защиту информации (как правило, подразделения ИТ и ИБ) и за служебное делопроизводство (режимные подразделения).

Ссылки

- Положение о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от её утечки по техническим каналам. Введено в действие постановлением Совета Министров – Правительства РФ от 15 сентября 1993 года № 912-51;
- Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти. Утверждено постановлением Правительства Российской Федерации от 03 ноября 1994 г. № 1233;
- Типовые требования к содержанию и порядку разработки Руководства по защите информации от технических разведок и от её утечки по техническим каналам. Одобрено решением Гостехкомиссии России от 03 октября 1995 г. № 42;
- ГОСТ Р 51583-2000 «Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения» (для служебного пользования);
- Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну. Утверждена приказом ФАПСИ России от 13 июня 2001 г. № 152;
- Руководящий документ «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)». Утверждён приказом Гостехкомиссии России от 30 августа 2002 г. № 282 (для служебного пользования);
- Постановление Правительства РФ от 15 августа 2006 г. № 504 «О лицензировании деятельности по технической защите конфиденциальной информации»;
- Постановление Правительства РФ от 29 декабря 2007 г. № 957 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами»;

- Методический документ «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных», ФСТЭК России, 15 февраля 2008 г. (пометка «для служебного пользования» снята решением ФСТЭК России от 16 ноября 2009 г.);
- Методический 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 обработке в информационных системах персональных данных». Утвержден руководством 8 Центра ФСБ России 21 февраля 2008 г. № 149/6/6-622;
- Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

Шаг 2.
Определить состав обрабатываемых ПДн, цели и условия обработки.
Определить срок хранения ПДн

Введение

Для того, чтобы наиболее эффективно спланировать деятельность по приведению процессов, в рамках которых происходит обработка ПДн, в соответствие требованиям нормативно-правовых актов Российской Федерации, необходимо обеспечить чёткое представление о том, какие именно категории информации ограниченного распространения используются оператором в производственной деятельности, на каких условиях и с какой целью осуществляется их обработка. Это достигается разработкой перечня сведений конфиденциального характера (перечня персональных данных), обрабатываемых оператором.

Цели проведения работ

Целью этапа является закрепление представления о составе, условиях и целях обработки персональных данных, формирование основы для дальнейшего планирования работ по приведению процессов, в рамках которых происходит обработка персональных данных, в соответствие требованиям нормативно-правовых актов Российской Федерации, регламентирующих порядок обработки ПДн.

Документированным выражением данного представления для оператора ПДн является Перечень персональных данных – подробный, четко структурированный документ, содержащий информацию обо всех категориях и видах персональных данных, обрабатываемых в организации с применением средств автоматизации или без такового, достаточный для:

- принятия решения о защите ПДн при их обработке в ИСПДн с применением средств автоматизации или без такового;
- определения максимальной категории ПДн, обрабатываемых в ИСПДн;
- разработки требований к системе защиты;
- определения условий и порядка начала и прекращения обработки ПДн и передачи их третьим лицам;
- определения степени ущерба, который может быть нанесен субъекту вследствие реализации возможных угроз безопасности ПДн.

Основание проведения работ

Требования по разработке подобного перечня оператором изложены в руководящих и методических документах ФСТЭК России.

Согласно руководящему документу «Специальные требования и рекомендации по технической защите конфиденциальной информации» (СТР-К), п. 3.6, в организации

должен быть документально оформлен перечень сведений конфиденциального характера, подлежащих защите в соответствии с нормативными правовыми актами, а также разработана соответствующая разрешительная система доступа персонала к такого рода сведениям.

Согласно методическому документу ФСТЭК России «Основные мероприятия по организации и техническому обеспечению безопасности ПДн, обрабатываемых в информационных системах персональных данных», в числе прочих мероприятий на предпроектной стадии определяется перечень ПДн, подлежащих защите от НСД.

Выполняемые работы

Для составления Перечня должен привлекаться широкий круг экспертов и должностных лиц структурных подразделений, отделов, служб организации с тем, чтобы ни одно из возможных направлений её деятельности не было упущено при его разработке. В ходе подготовки Перечня должностные лица организации, а в случае проведения работ сторонней организацией – сотрудники организации-исполнителя должны провести анализ всех сторон деятельности оператора с целью определения конкретных сведений, разглашение которых может нанести ущерб их собственнику и владельцу (субъекту персональных данных).

При этом выполняются следующие работы:

- изучение внутренней и внешней организационно-распорядительной документации;
- интервьюирование должностных лиц и специалистов оператора;
- идентификация точек входа и выхода информации ограниченного распространения и пути её миграции в структуре оператора;
- изучение содержания входящих и исходящих информационных потоков всех типов и направлений;
- выявление в информационных потоках, сопровождающих бизнес-процессы оператора, персональных данных и других видов информации ограниченного распространения, обрабатываемых как с использованием, так и без использования средств автоматизации;
- анализ оснований и установление категорий и степеней конфиденциальности выявленных персональных данных и других видов информации ограниченного распространения, циркулирующих в структуре оператора;
- уточнение целей, выявление условий начала и прекращения и определение сроков обработки (хранения) для каждой установленной категории персональных данных и другой информации ограниченного распространения;
- определение структурных подразделений и должностных лиц оператора, использующих в своей деятельности персональные данные и другую информацию ограниченного распространения, их правомочности в принятии решений, касающихся определения целей, условий и сроков обработки указанной информации;
- составление и представление на утверждение Перечня сведений конфиденциального характера (Перечня персональных данных), отвечающего

требованиям руководящих документов и содержащего информацию, необходимую и достаточную для достижения целей работ.

Результат

В результате данного шага оператор получает сформированное мнение о составе и содержании обрабатываемых в его структуре персональных данных и другой информации ограниченного распространения, оформленное в виде Перечня сведений конфиденциального характера (Перечня персональных данных) и приказа о его введении в действие. Данным приказом могут быть определены порядок и правила использования Перечня в тех или иных бизнес-процессах, требования по его доведению до сотрудников организации-оператора, клиентов и прочих физических и юридических лиц.

В результате работ ответственные за организацию и обеспечение безопасности ПДн получают возможность спланировать дальнейшие работы по приведению процессов организации, связанных с обработкой ПДн, в соответствие требованиям закона № 152-ФЗ.

Ограничения / на что стоит обратить внимание

Наиболее информативными источниками получения исходных данных для формирования Перечня могут быть процессы:

- оформления трудовых договоров с работниками;
- ведения учёта труда работников и их оплаты;
- осуществления обязательного государственного пенсионного страхования работников;
- осуществления обязательного пенсионного страхования в негосударственном пенсионном фонде;
- продажи товаров дистанционным способом;
- оказания услуг связи;
- оказания услуг по обязательному (добровольному) медицинскому страхованию граждан;
- оказания банковских услуг;

и др.

В ходе формирования Перечня должны быть обеспечены единый подход к созданию Перечня со стороны всех структурных подразделений организации и привлекаемых сотрудников, обоснованность принимаемых решений о включении в него сведений за структурное подразделение в отдельности и за организацию в целом, а также воспитание чувства ответственности за их несанкционированное распространение (разглашение, передачу, опубликование, утечку, хищение) вплоть до применения соответствующих норм Гражданского кодека Российской Федерации (ГК РФ), Кодекса Российской Федерации об административных правонарушениях (КоАП) и Уголовного кодекса Российской Федерации (УК РФ).

В Перечень должны включаться сведения, содержащие информацию ограниченного распространения (персональные данные), не составляющую государственную тайну, – как являющиеся собственностью организации, так и передаваемые (предоставляемые) в

распоряжение (пользование) организации органами исполнительной власти, государственными учреждениями и организациями, а также любыми другими организациями, предприятиями и субъектами (физическими лицами), с которыми установлены договорные отношения, предусматривающие обязательства по неразглашению конфиденциальной информации.

Следует особое внимание уделять обоснованию целей обработки всех категорий информации ограниченного распространения. Совмещение в одной ИСПДн персональных данных с различными целями обработки недопустимо. Так, согласно части 2 статьи 5 федерального закона хранение персональных данных должно осуществляться не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении. А в соответствии частью 4 статьи 21 закона обработка персональных данных по достижении целей обработки должна быть прекращена в срок не менее трёх рабочих дней, если иное не предусмотрено федеральными законами.

Так, согласно Перечню типовых управленческих документов, сопровождающих деятельность организаций с указанием сроков хранения, утверждённому Росархивом 6 октября 2000 г., многие документы кадрового делопроизводства, содержащие персональные данные, должны храниться 75 лет.

Ссылки

- Руководящий документ «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)». Утвержден приказом Гостехкомиссии России от 30 августа 2002 г. № 282 (для служебного пользования);
- Методический документ «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных», ФСТЭК России, 15 февраля 2008 г. (пометка «для служебного пользования» снята решением ФСТЭК России от 16 ноября 2009 г.).

Шаг 3.
Получить согласие субъекта на обработку его ПДн, в том числе в письменной форме

Введение

Одним из условий обработки персональных данных является её осуществление с согласия субъекта персональных данных, за исключением случаев, предусмотренных частью 2 статьи 6 федерального закона № 152-ФЗ.

Невыполнение условия согласия субъекта на обработку его персональных данных может привести к нарушению конституционных прав субъекта вследствие вмешательства в его личную жизнь путём осуществления контактов с ним по различным поводам без его на то согласия (например – рассылка персонифицированных рекламных предложений и т.п.).

Для обеспечения защиты законных прав и свобод субъекта на неприкосновенность частной жизни необходимо исключить случаи, когда обработка персональных данных прямо или косвенно нарушает эти права. В этих целях рекомендуется провести ряд мероприятий, направленных на получение согласия субъектов персональных данных, чьи данные уже обрабатываются, и разработать схему для штатного получения таких согласий в будущем.

Цели проведения работ

Цели данного этапа:

- проверить наличие юридически значимого согласия субъектов персональных данных на обработку персональных данных, выявленных на Шаге 2;
- получить согласие на обработку персональных данных от субъектов, согласие которых на обработку которых должно быть получено, но не было обнаружено в ходе проверки;
- разработать и ввести в действие процедуры, связанные с получением и использованием согласия субъектов персональных данных на обработку их персональных данных оператором;
- сформировать юридически значимые доказательные базы для обоснования легитимности обработки персональных данных.

Основание проведения работ

В соответствии с частью 1 статьи 6 Федерального закона № 152-ФЗ, обработка персональных данных может осуществляться оператором с согласия субъектов персональных данных, за исключением случаев, предусмотренных частью 2 той же статьи.

Согласно части 2 статьи 6, согласия субъекта на обработку его персональных данных не требуется в случаях, когда:

- обработка персональных данных осуществляется на основании федерального закона, устанавливающего её цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора;
- обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных;
- обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;
- обработка персональных данных необходима для доставки почтовых отправлений организациями почтовой связи, для осуществления операторами электросвязи расчетов с пользователями услуг связи за оказанные услуги связи, а также для рассмотрения претензий пользователей услугами связи;
- обработка персональных данных осуществляется в целях профессиональной деятельности журналиста либо в целях научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и свободы субъекта персональных данных;
- осуществляется обработка персональных данных, подлежащих опубликованию в соответствии с федеральными законами, в том числе персональных данных лиц, замещающих государственные должности, должности государственной гражданской службы, персональных данных кандидатов на выборные государственные или муниципальные должности.

Во всех других случаях необходимо провести комплекс мероприятий по получению согласия на обработку персональных данных.

Согласно части 1 статьи 9 закона, субъект персональных данных принимает решение о предоставлении своих персональных данных и даёт согласие на их обработку своей волей и в своем интересе, за исключением случаев, предусмотренных частью 2 той же статьи. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных.

Законом установлен ряд случаев, когда согласие субъекта на обработку его персональных данных должно быть дано исключительно в письменной форме или когда отсутствие письменного подтверждения согласия приводит к невозможности принятия решения, порождающего юридические последствия в отношении субъекта персональных данных. Доказательной базой наличия согласия субъекта на обработку его персональных данных могут быть только официальные, юридически грамотно оформленные документы.

Таким образом, отсутствие доказательств, подтверждающих право оператора на обработку ПДн в тех случаях, когда отсутствуют основания для обработки ПДн без согласия субъекта, а также продолжение такой обработки после отзыва субъектом своего согласия может быть расценено как нарушение федерального закона и привести к неприемлемым последствиям для субъекта персональных данных.

Выполняемые работы

Учитывая сформированное при выполнении работ по Шагу 2 представление о составе, условиях и целях обработки персональных данных, на текущем шаге выделяются следующие блоки ПДн, обработка которых осуществляется оператором:

- ПДн, согласие на обработку которых имеется;
- ПДн, на обработку которых согласие необходимо, но отсутствует;
- ПДн, подлежащие опубликованию в соответствии с законом;
- прочие ПДн, согласия субъектов на обработку которых не требуется в соответствии счастью 2 статьи 6 федерального закона № 152-ФЗ «О персональных данных».

В соответствии с данными блоками выполняемые работы включают в себя:

- анализ состава и содержания документов, подтверждающих легитимность обработки оператором персональных данных, в отдельности для каждого из субъектов, чьи ПДн обрабатываются оператором;
- идентификацию субъектов персональных данных, чьё разрешение на обработку их ПДн отсутствует, и принятие решения о необходимости или об отсутствии необходимости получения такого разрешения;
- разработку (корректировку) договоров с сотрудниками и клиентами организации-оператора в части внесения в них положений об условиях и формах обработки ПДн оператором и о согласии на такую обработку;
- разработку типовых форм согласия и направление запросов субъектам для получения их согласия на обработку их ПДн оператором;
- организацию юридически значимого получения согласия через web-формы;
- формирование юридически значимой базы согласий субъектов на обработку их ПДн;
- разработку процедур и порядка реагирования на отсутствие ответа от субъекта, подтверждающего его согласие на обработку его ПДн;
- разработку процедур и порядка реагирования на отзыв субъектом своего согласия на обработку его ПДн;
- идентификацию ПДн, подлежащих опубликованию в соответствии с федеральными законами, в инфраструктуре оператора;
- установление наличия или отсутствия целей обработки персональных данных, подлежащих опубликованию в соответствии с федеральными законами, в инфраструктуре оператора, направление субъектам при необходимости запросов о предоставлении таких ПДн для обработки оператором;
- идентификацию прочих ПДн, согласия субъектов на обработку которых не требуется в соответствии с частью 2 статьи 6 федерального закона № 152-ФЗ «О персональных данных»;
- формирование документированной, юридически значимой доказательной базы правомерности обработки ПДн, осуществляемой без согласия субъекта персональных данных.

Результат

Результаты данного этапа:

- выявлены персональные данные, по которым согласие уже получено или не требуется;
- проведены мероприятия по получению юридически значимого письменного согласия на обработку ПДн в тех случаях, когда такое согласие получено не было;
- разработаны процедуры и порядок действий оператора, связанных с получением согласия субъектов на обработку их ПДн;
- сформированы юридически значимые базы письменных согласий субъектов на обработку их ПДн;
- сформирована юридически значимая доказательная база правомерности обработки ПДн, осуществляемой без согласия субъекта персональных данных.

Ограничения / на что стоит обратить внимание

Особенно важной является аналитическая проработка и создание юридически значимой доказательной базы правомерности обработки ПДн, осуществляемой без согласия субъекта персональных данных. Как показывает практика, таких случаев достаточно много, и качественная аналитическая проработка данного блока ПДн позволяет значительно снизить издержки на разработку и исполнение процедуры получения согласия.

Необходимо также обратить внимание на то, что согласно закону № 152-ФЗ «О персональных данных» в большинстве случаев от субъекта необходимо получить именно письменное согласие. Согласно части 4 статьи 9 закона, письменное согласие субъекта персональных данных на обработку персональных данных должно включать в себя:

- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных;
- цель обработки ПДн;
- перечень ПДн, на обработку которых дается согласие субъекта персональных данных;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки ПДн;
- срок, в течение которого действует согласие, а также порядок его отзыва.

Для упрощения и повышения эффективности мероприятий по получению согласия субъектов на обработку их ПДн могут быть предложены следующие процедуры:

- направление в адрес субъекта персональных данных письма с просьбой подписать согласие на обработку его ПДн в адрес субъекта. К письму рекомендуется приложить заполненную типовую форму согласия и конверт с заполненным обратным адресом;

- направление в адрес субъекта письма с просьбой посетить офис компании с целью подписания согласия;
- направление на почтовый и электронный адреса субъекта разъяснений о порядке предоставления своего согласия на обработку ПДн через web-формы и предложения предоставить своё согласие данным способом. Критерием, свидетельствующим о получении оператором согласия субъекта персональных данных на обработку его ПДн, может служить файл электронной цифровой подписи. Кроме того, оператор вправе ввести в web-форму заявки дополнительные поля, обязательные для заполнения, устанавливающие условие согласия субъекта персональных данных на обработку его ПДн, при условии последующего проведения мероприятий по проверке достоверности представленных ПДн;

и др.

Субъект персональных данных должен быть предупрежден о том, что игнорирование обращений к нему со стороны оператора может быть расценено как его согласие на обработку его персональных данных оператором.

Ссылки

- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных», ст. 6 ч. 2; ст. 8 ч.ч. 1, 4; ст. 9; ст. 11 ч. 1; ст. 15 ч. 1; ст. 16 ч. 2; ст. 21 ч. 5; ст. 22 ч. 2;
- Трудовой кодекс Российской Федерации от 30 декабря 2001 г. № 197-ФЗ, ст. 86, ст. 88, ст. 89;
- Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», разд. 2, ст. 6.

Шаг 4.
Определить порядок реагирования на запросы со стороны субъектов персональных данных

Введение

Основной целью Федерального закона № 152-ФЗ «О персональных данных» является защита прав субъектов персональных данных, поэтому в нём четко определены права субъектов персональных данных и соответствующие обязанности оператора, а именно:

- оператор должен предоставлять субъекту персональных данных сведения о его персональных данных в установленном формате;
- оператор должен блокировать ПДн в ряде случаев, предусмотренных законом;
- оператор должен уничтожать ПДн в ряде случаев, предусмотренных законом.

Невыполнение требований закона по предоставлению гражданину информации о содержании, условиях обработки его ПДн, другой информации, затрагивающей его законные права и интересы, может быть квалифицировано как правонарушение, предусмотренное статьёй 5.39 Кодекса Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ либо статьёй 140 Уголовного кодекса Российской Федерации от 13 июня 1996 г. № 63-ФЗ и повлечь соответствующую ответственность.

Ниже описаны рекомендуемые к проведению оператором мероприятия, направленные на организацию процесса реагирования на запросы субъектов персональных данных в соответствии с требованиями законодательства.

Цели проведения работ

Основной целью проведения работ на данном шаге является определение порядка реагирования на запросы субъектов персональных данных и разработка описывающих его регламентов для сведения к минимуму вероятности нарушения прав субъектов при обработке их ПДн предприятием-оператором.

Основание проведения работ

Основанием для проведения работ являются требования Федерального закона № 152-ФЗ «О персональных данных», а именно:

> *Ст. 20, ч. 1: Оператор обязан в порядке, предусмотренном статьей 14 настоящего Федерального закона, сообщить субъекту персональных данных или его законному представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных…*
>
> *Ст. 20, ч. 3: Оператор обязан безвозмездно предоставить субъекту персональных данных или его законному представителю возможность ознакомления с персональными данными, относящимися к соответствующему субъекту*

персональных данных, а также внести в них необходимые изменения, уничтожить или блокировать соответствующие персональные данные по предоставлении субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные, которые относятся к соответствующему субъекту и обработку которых осуществляет оператор, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки...

Ст. 21, ч. 3: В случае выявления неправомерных действий с персональными данными оператор в срок, не превышающий трёх рабочих дней с даты такого выявления, обязан устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений оператор в срок, не превышающий трёх рабочих дней с даты выявления неправомерности действий с персональными данными, обязан уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных или его законного представителя...

Ст. 21, ч 4: В случае достижения цели обработки персональных данных оператор обязан незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные в срок, не превышающий трёх рабочих дней с даты достижения цели обработки персональных данных, если иное не предусмотрено федеральными законами, и уведомить об этом субъекта персональных данных или его законного представителя...

Ст. 21, ч. 5: В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных оператор обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий трёх рабочих дней с даты поступления указанного отзыва.

Выполняемые работы

Для достижения целей данного этапа необходимо провести следующие работы:

- определить лиц, ответственных за соблюдение требований № 152-ФЗ «О персональных данных» в части реагирования на запросы субъектов персональных данных;
- разработать механизмы реагирования на запросы субъектов персональных данных (например, документальные регламенты или процедуры);
- ввести в действие в рамках организации-оператора разработанные регламенты реагирования на запросы субъектов персональных данных;
- разработать типизированные шаблоны ответов на запросы субъектов персональных данных;
- провести мероприятия по проверке выполнения разработанных механизмов реагирования на запросы субъектов персональных данных.

Регламенты реагирования направлены на сведение к минимуму риска нарушения прав субъектов персональных данных при поступлении от них запросов от субъекта

персональных данных, а также при наступлении факта достижения целей обработки ПДн и отзыва согласия субъекта персональных данных на обработку его ПДн.

Регламенты реагирования должны содержать следующие сведения:

- лицо (список лиц), ответственных за получение запросов субъектов персональных данных;
- порядок проверки корректности сведений указанных в форме запроса субъекта персональных данных;
- порядок формирования ответа на запрос субъекта персональных данных;
- порядок внесения в ПДн уточняющих и/или корректирующих сведений, полученных от субъекта персональных данных;
- лицо (список лиц), ответственных за определение фактов достижения целей обработки ПДн;
- порядок блокирования и/или уничтожения ПДн при наступлении факта достижения цели обработки ПДн;
- лицо (список лиц), ответственных за контроль наличия согласий субъектов персональных данных, а также за получение отзыва согласия субъектов персональных данных;
- порядок блокирования и/или уничтожения ПДн при отзыве согласия субъекта персональных данных.

Результат

Результатом выполненных работ являются введенные в действие в рамках организации-оператора эффективные механизмы реагирования на запросы субъектов персональных данных.

Документированным выражением полученного результата являются:

- регламенты, процедуры, инструкции и прочие документы системы внутренней организационно-распорядительной документации организации-оператора, устанавливающие порядок реагирования на запросы со стороны субъектов персональных данных;
- приказы руководителя о введении разработанных организационно-распорядительных документов в действие;
- документы, подтверждающие факты доведения разработанных организационно-распорядительных документов до персонала и обеспечения контроля над их исполнением.

Ограничения / на что стоит обратить внимание

При разработке регламентов реагирования необходимо обратить внимание на сроки, установленные в федеральном законе № 152-ФЗ «О персональных данных», а именно:

- оператор обязан сообщить субъекту персональных данных о наличии его ПДн в течение десяти рабочих дней с даты получения запроса субъекта персональных данных или его законного представителя;
- в случае отказа в предоставлении субъекту персональных данных информации оператор обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 5 статьи 14 настоящего Федерального закона или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий семи рабочих дней со дня обращения субъекта персональных данных;
- оператор обязан сообщить в уполномоченный орган по защите прав субъектов персональных данных по его запросу информацию, необходимую для осуществления деятельности указанного органа, в течение семи рабочих дней с даты получения такого запроса;
- в случае выявления неправомерных действий с персональными данными оператор в срок, не превышающий трёх рабочих дней с даты такого выявления, обязан устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений оператор в срок, не превышающий трёх рабочих дней с даты выявления неправомерности действий с персональными данными, обязан уничтожить указанные персональные данные;
- в случае отзыва субъектом персональных данных согласия на обработку своих ПДн оператор обязан прекратить обработку ПДн и уничтожить их в срок, не превышающий трёх рабочих дней с даты поступления указанного отзыва.

При разработке процедуры ответа на запросы субъектов персональных данных следует учитывать предоставленные субъектам частью 4 статьи 14 федерального закона № 152-ФЗ права на получение информации, касающейся обработки его ПДн, в том числе содержащей:

- подтверждение факта обработки персональных данных оператором, а также цель такой обработки;
- способы обработки персональных данных, применяемые оператором;
- сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
- перечень обрабатываемых персональных данных и источник их получения;
- сроки обработки персональных данных, в том числе сроки их хранения;
- сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

Федеральный закон № 152-ФЗ «О персональных данных» накладывает ограничения на права субъектов персональных данных в ряде случаев:

ст. 14, п. 5: Право субъекта персональных данных на доступ к своим персональным данным ограничивается в случае, если:

1) *обработка персональных данных, в том числе персональных данных, полученных в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;*
2) *обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении*

преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;

3) *предоставление персональных данных нарушает конституционные права и свободы других лиц.*

Ссылки

- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных», ст. 4 ч. 6; ст. 14 ч.ч. 4, 5; ст. 20 ч.ч. 1, 3; ст. 21 ч.ч. 3…5;
- Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ, ст. 5.39;
- Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ, ст. 140.

Шаг 5.

Определить необходимость уведомления уполномоченного органа по защите ПДн о начале обработки ПДн. Если необходимость есть, то составить и отправить уведомление

Введение

Одним из условий обработки персональных данных является необходимость уведомить уполномоченный орган по защите прав субъектов персональных данных (в настоящее время – Роскомнадзор) о своем намерении осуществлять обработку ПДн. Исключение составляют случаи, предусмотренные частью 2 статьи 22 федерального закона № 152-ФЗ.

Невыполнение условия уведомления уполномоченного органа может быть квалифицировано как правонарушение, предусмотренное статьёй 19.7 Кодекса Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ и повлечь соответствующую ответственность.

В целях снижения риска нарушений требований закона, влекущих ответственность по указанной статье, необходимо убедиться в наличии или отсутствии у организации-оператора оснований не подавать уведомление об обработке ПДн в уполномоченный орган по защите прав субъектов персональных данных. В случае если выявлен хотя бы один факт обработки ПДн, не подпадающий под перечень случаев, предусмотренных частью 2 статьи 22 федерального закона № 152-ФЗ, уведомление должно быть подготовлено и отправлено.

Цели проведения работ

Цели данного этапа:

- определить необходимость подачи уведомления об обработке персональных данных в уполномоченный орган по защите прав субъектов персональных данных;
- подготовить правовое обоснование отсутствия необходимости подачи уведомления об обработке ПДн, если все обрабатываемые ПДн подпадают под исключения, предусмотренные частью 2 статьи 22 Федерального закона № 152-ФЗ;
- в случае необходимости, подготовить уведомление об обработке ПДн в соответствии с требованиями регулятора и отправить в уполномоченный орган.

Основание проведения работ

Работы выполняются на основании части 1 статьи 22 Федерального закона № 152-ФЗ.

> *Ст. 22, ч. 1: Оператор до начала обработки персональных данных обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи.*

Согласно части 2 статьи 22 федерального закона № 152-ФЗ, оператор вправе осуществлять обработку без уведомления уполномоченного органа по защите прав субъектов персональных данных следующих персональных данных:

- относящихся к субъектам персональных данных, которых связывают с оператором трудовые отношения;
- полученных оператором в связи с заключением договора, стороной которого является субъект персональных данных, если его ПДн не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;
- относящихся к членам (участникам) общественного объединения или религиозной организации и обрабатываемых соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что ПДн не будут распространяться без согласия субъектов персональных данных, данного в письменной форме;
- являющихся общедоступными персональными данными;
- включающих в себя только фамилии, имена и отчества субъектов персональных данных;
- необходимых в целях однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях;
- включенных в ИСПДн, имеющие в соответствии с федеральными законами статус федеральных автоматизированных информационных систем, а также в государственные ИСПДн, созданные в целях защиты безопасности государства и общественного порядка;
- обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности ПДн при их обработке и к соблюдению прав субъектов персональных данных.

При обработке иных ПДн необходимо подготовить и отправить в уполномоченный орган по защите прав субъектов персональных данных соответствующее уведомление.

Выполняемые работы

Используя представление о составе, условиях и целях обработки ПДн, сформированное при разработке перечня сведений конфиденциального характера (см. Шаг 2), на текущем шаге необходимо проанализировать всю совокупность обрабатываемых в организации персональных данных, по всем сотрудникам организации, клиентам, партнерам и прочим физическим и юридическим лицам, чьи персональные данные обрабатываются организацией-оператором в той или иной форме, на предмет возможности применения к ним исключений, предусмотренных частью 2 статьи 22 Федерального закона № 152-ФЗ.

После определения подходящего пункта исключения необходимо подготовить правовое обоснование применимости данного исключения к данной категории (виду, пункту перечня) ПДн для организации-оператора, подтвержденное соответствующими фактами (договорами, согласиями и т.п.).

Если же в проанализированной совокупности обрабатываемых данных имеется хотя бы один элемент, не подпадающий под указанные исключения, необходимо соответствующим образом оформить уведомление и отправить его в территориальный орган Роскомнадзора.

При подготовке уведомления необходимо опираться на приказы и рекомендации Роскомнадзора, размещенные на ведомственном сайте http://www.rsoc.ru/personal-data/p181/. К таким документам относятся:

- форма уведомления об обработке (о намерении осуществлять обработку) персональных данных;
- рекомендации по заполнению образца формы уведомления об обработке (о намерении осуществлять обработку) персональных данных.

Также есть возможность заполнить электронную форму уведомления и распечатать его на корпоративном бланке. При заполнении электронной формы уведомления необходимо учитывать, что подача его в электронном виде в Роскомнадзор не является достаточной процедурой. Помимо подачи уведомления в электронной форме необходимо подготовить и отправить уведомление на бумажном носителе за подписью руководителя организации-оператора.

Уведомление должно содержать следующие сведения:

- наименование (фамилия, имя, отчество), адрес оператора;
- цель обработки персональных данных;
- категории персональных данных;
- категории субъектов, персональные данные которых обрабатываются;
- правовое основание обработки персональных данных;
- перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных;
- описание мер, которые оператор обязуется осуществлять при обработке персональных данных, по обеспечению безопасности персональных данных при их обработке;
- дата начала обработки персональных данных;
- срок или условие прекращения обработки персональных данных.

Результат

Результаты данного этапа:

- Определена необходимость подачи уведомления об обработке персональных данных в уполномоченный орган по защите прав субъектов персональных данных;
- Подготовлено правовое обоснование отсутствия необходимости подачи уведомления об обработке ПДн, если все обрабатываемые персональные данные

подпадают под исключения, предусмотренные частью 2 статьи 22 Федерального закона № 152-ФЗ;

- В случае выявления необходимости, подготовлено и отправлено уведомление об обработке ПДн в соответствии с требованиями регулятора.

Ограничения / на что стоит обратить внимание

Особенно важной является аналитическая проработка правового обоснования отсутствия необходимости подачи уведомления об обработке ПДн. Как показывает практика, таких случаев достаточно много, и качественная аналитическая проработка данной части этапа позволяет избежать уведомления уполномоченного органа по защите прав субъектов персональных данных, а, следовательно, снизить вероятность возникновения претензий регулирующих органов. Например, необходимо обратить внимание на первые два пункта части 2 статьи 22 Федерального закона № 152-ФЗ, которые наиболее часто позволяют обрабатывать персональные данные без уведомления уполномоченного органа. Согласно этим пунктам оператор не обязан уведомлять уполномоченный орган в случае, если персональные данные:

- относятся к субъектам персональных данных, которых связывают с оператором трудовые отношения;
- получены оператором в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных.

Организация-оператор, подающая уведомление об обработке ПДн, должна иметь в виду, что в случае предоставления неполных или недостоверных сведений уполномоченный орган вправе требовать от оператора уточнения предоставленных сведений до их внесения в реестр операторов.

В случае изменения сведений оператор обязан уведомить об этом уполномоченный орган в течение десяти рабочих дней с даты их возникновения.

Уполномоченный орган по защите прав субъектов персональных данных имеет право осуществлять проверку сведений, содержащихся в уведомлении об обработке персональных данных, или привлекать для осуществления такой проверки иные государственные органы в пределах их полномочий (см. часть 3 статьи 23 федерального закона № 152-ФЗ).

Уполномоченный орган по защите прав субъектов персональных данных в течение тридцати дней с даты поступления уведомления вносит сведения, указанные в части 3 статьи 22 федерального закона № 152-ФЗ, в реестр операторов. Эти сведения, за исключением сведений о средствах обеспечения безопасности персональных данных при их обработке, являются общедоступными.

Ссылки

- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных», ст. 22;
- Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ, ст. 19.7;
- Приказ Россвязьохранкультуры от 28 марта 2008 г. № 154 «Об утверждении Положения о ведении реестра операторов, осуществляющих обработку персональных данных»;
- Приказ Россвязькомнадзора от 17 июля 2008 г. № 8 «Об утверждении образца формы уведомления об обработке персональных данных»;
- Форма уведомления об обработке (о намерении осуществлять обработку) персональных данных (Приложение № 1 к приказу Россвязькомнадзора от 17 июля 2008 г. № 8);
- Рекомендации по заполнению образца формы уведомления об обработке (о намерении осуществлять обработку) персональных данных (Приложение № 2 к приказу Россвязькомнадзора от 17 июля 2008 г. № 8);
- Приказ Россвязькомнадзора от 18 февраля 2009 г. № 42 «О внесении изменений в приказ Россвязькомнадзора от 17 июля 2008 г. № 8 «Об утверждении образца формы уведомления об обработке персональных данных».

Шаг 6.
Выделить и классифицировать ИСПДн

Введение

Классификация ИСПДн является обязательной процедурой, осуществляемой с учётом категорий и объёма накапливаемых, обрабатываемых и распределяемых с их использованием ПДн. Классификация ИСПДн – основное условие корректного установления методов и средств защиты, необходимых для обеспечения безопасности ПДн.

Классификации ИСПДн предшествует их идентификация.

Цели проведения работ

Целями данного этапа являются:

- выделение (идентификация) и определение состава ИСПДн, имеющихся в ИТ-инфраструктуре предприятия;
- классификация ИСПДн в соответствии с нормативно-правовыми актами Минкомсвязи, ФСТЭК России и ФСБ России;
- разработка первого комплекта обязательных документов для каждой идентифицированной ИСПДн.

Основание проведения работ

В соответствии с пунктом 6 «Положения об обеспечении безопасности ПДн при их обработке в ИСПДн» (утв. постановлением Правительства Российской Федерации от 17 ноября 2007 г. № 781), ИСПДн подлежат классификации. Порядок проведения классификации устанавливается совместно Федеральной службой по техническому и экспортному контролю, Федеральной службой безопасности Российской Федерации и Министерством информационных технологий и связи Российской Федерации.

В соответствии с требованиями данного пункта изданы следующие руководящие и методические документы, подлежащие исполнению при проведении работ:

- Приказ ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных»;
- Методический документ «Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», ФСТЭК России, 15 февраля 2008 г. (пометка «для служебного пользования» снята решением ФСТЭК России от 16 ноября 2009 г.);
- Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных

системах персональных данных с использованием средств автоматизации. ФСБ России, 21 февраля 2008 г, № 149/5-144.

Выполняемые работы

На данном этапе проводятся:

- идентификация ИСПДн – выделение в ИТ-инфраструктуре предприятия областей (отдельных рабочих станций, узлов и сегментов сети), в которых осуществляется обработка ПДн, определение границ контролируемых зон для выделенных областей, присвоение наименований отдельным ИСПДн в составе ИТ-инфраструктуры предприятия, утверждение перечня защищаемых ИСПДн приказом руководителя предприятия;
- классификация ИСПДн – присвоение каждой идентифицированной ИСПДн класса (К1, К2, К3, К4), соответствующего её индивидуальным признакам, с составлением акта классификации каждой ИСПДн.

Идентификация ИСПДн включает в себя следующие блоки работ:

Изучение бизнес-процессов

Необходимо идентифицировать и описать бизнес-процессы, связанные с обработкой ПДн. Определить, с помощью каких программных и технических средств реализуется каждый из этих процессов.

Составление схемы сети

Необходимо составить функциональную схему корпоративной сети организации, на которой отметить технические средства, задействованные в обработке ПДн, и показать линии связи, по которым осуществляется передача ПДн.

Составление карты сети

Необходимо составить карту сети, на которой указать помещения, серверы, АРМ, прочие технические средства, используемые для обработки ПДн, места прокладки линий, по которым передаётся защищаемая информация.

Сегментация сети

Используя представление о бизнес-процессах, схему и карту сети, необходимо выделить в инфраструктуре сети отдельные совокупности технических средств – сегменты сети, в каждом из которых:

- обрабатываются исключительно свойственные для данной совокупности технических средств категории ПДн;
- ставятся цели обработки ПДн, отличные от целей обработки ПДн в других сегментах сети.

Каждый выделенный таким образом сегмент сети может представлять собой отдельную ИСПДн. В случае отделения от остальной сети сертифицированным межсетевым экраном соответствующего класса, данная ИСПДн может быть классифицирована отдельно от других (см. ниже).

Принятие решения

На основе сегментации идентифицируются все ИСПДн, существующие в ИТ-инфраструктуре организации.

Необходимо помнить, что в случае объединения двух ИСПДн, которые имеют различные классы, класс объединённой системы должен быть не ниже, чем наивысший класс одной из объединяемых систем. Исключением является случай их объединения посредством сертифицированного межсетевого экрана (МЭ) соответствующего класса, когда каждая из объединяющихся ИСПДн может сохранять свой класс защищённости.

Решение должно быть обосновано путем сравнения затрат на создание и эксплуатацию СЗПДн сети в целом с затратами на создание и эксплуатацию нескольких обособленных сегментов защиты, поскольку для их создания требуется закупка и установка сертифицированных межсетевых экранов.

Классификация ИСПДн предусматривает проведение следующих мероприятий:

Назначение комиссии

Для проведения классификации ИСПДн приказом по предприятию назначается комиссия и её председатель. В состав комиссии включаются руководители (представители) подразделений, осуществляющих обработку персональных данных, сотрудники ИТ- и ИБ-подразделений предприятия.

Изучение классификационных признаков

Признаки ИСПДн, влияющие на определение её класса, подробно описаны в «Порядке проведения классификации информационных систем персональных данных», утверждённом приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 г. № 55/86/20.

Разработка и утверждение Акта классификации

Акт классификации должен соответствовать рекомендованной руководящим документом СТР-К форме и содержать в себе:

- основание для проведения классификации;
- точное наименование и место дислокации ИСПДн;
- перечень классификационных признаков ИСПДн и её характеристик, влияющих на определение класса;
- решение комиссии об установлении класса.

Акт классификации подписывается председателем комиссии и её членами и утверждается руководителем организации.

Результат

Результатом этапа являются комплекты текстовых и графических материалов, описывающих ИСПДн, а также обязательные для разработки Акты классификации на каждую идентифицированную ИСПДн.

Ограничения / на что стоит обратить внимание

В различных разделах «Порядка проведения классификации информационных систем персональных данных», утверждённого приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 г. № 55/86/20, а также в методических документах ФСТЭК России содержатся рекомендации по классификации ИСПДн, сущность которых необходимо понимать достаточно глубоко для того, чтобы избежать ошибок при определении класса.

В соответствии с последними рекомендациями ФСТЭК России, опубликованными на сайте ФСТЭК России http://www.fstec.ru/ razd/ ispo.htm, класс ИСПДн определяется с учётом категорий и объёма обрабатываемых ПДн, и независимо от того, является ли ИСПДн типовой или специальной, ей должен быть присвоен буквенно-цифровой индекс К1, К2, К3 или К4.

При наличии большого количества разноплановых классификационных признаков и в отсутствие четко сформулированного алгоритма классификации и разработки требований к системе защиты определение класса ИСПДн порой становится непростой аналитической задачей, требующей знания руководящих документов, применения специальных методологий и тщательного обследования информационной системы.

Классификация ИСПДн – не самоцель. Она необходима для последующей корректной разработки требований к системе защиты. И эти два процесса тесно связаны и взаимно зависят друг от друга. В наибольшей степени это относится к специальным ИСПДн, для которых обязательным условием является разработка Модели угроз и на её основе корректировка требований к системе защиты, определяемых согласно присвоенному классу.

Типовой алгоритм определения класса ИСПДн (см. рис. № 1) включает в себя не только вышеописанные работы, но и другие элементы, влияющие на этапе классификации ИСПДн на достижение целей построения эффективной, надежной и эргономичной системы защиты.

Необходимые исходные данные для идентификации и определения класса ИСПДн собираются на этапе предпроектного обследования объектов размещения информационных систем оператора. Именно на данном этапе производится изучение бизнес-процессов, связанных с обработкой ПДн, структуры сети, физических и логических связей между элементами и узлами сети, строятся функциональная схема и карта сети, проводится разделение сети на сегменты. На основании результатов изучения перечней защищаемых ресурсов, целей обработки ПДн и основных параметров технической и программной составляющих ИТ-инфраструктуры, условий расположения и других характеристик, и исходя из принятой в компании политики развития ИТ-инфраструктуры принимается решение об идентификации тех или иных сегментов сети как отдельных ИСПДн.

Далее в отдельности для каждой из идентифицированных ИСПДн определяются значения индексов $X_{ПД}$ (соответствует категории обрабатываемых в информационной системе персональных данных) и $X_{НПД}$ (зависит от объёма обрабатываемых в ИСПДн персональных данных). На основании значений данных индексов в соответствии с «Порядком проведения классификации информационных систем персональных данных»,

утверждённым приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 г. № 55/86/20, каждой ИСПДн присваивается класс К1, К2, К3 или К4.

Одновременно на основе анализа полученных данных и с использованием методических рекомендаций ФСТЭК России уточняются характеристики безопасности ИСПДн (типовая или специальная).

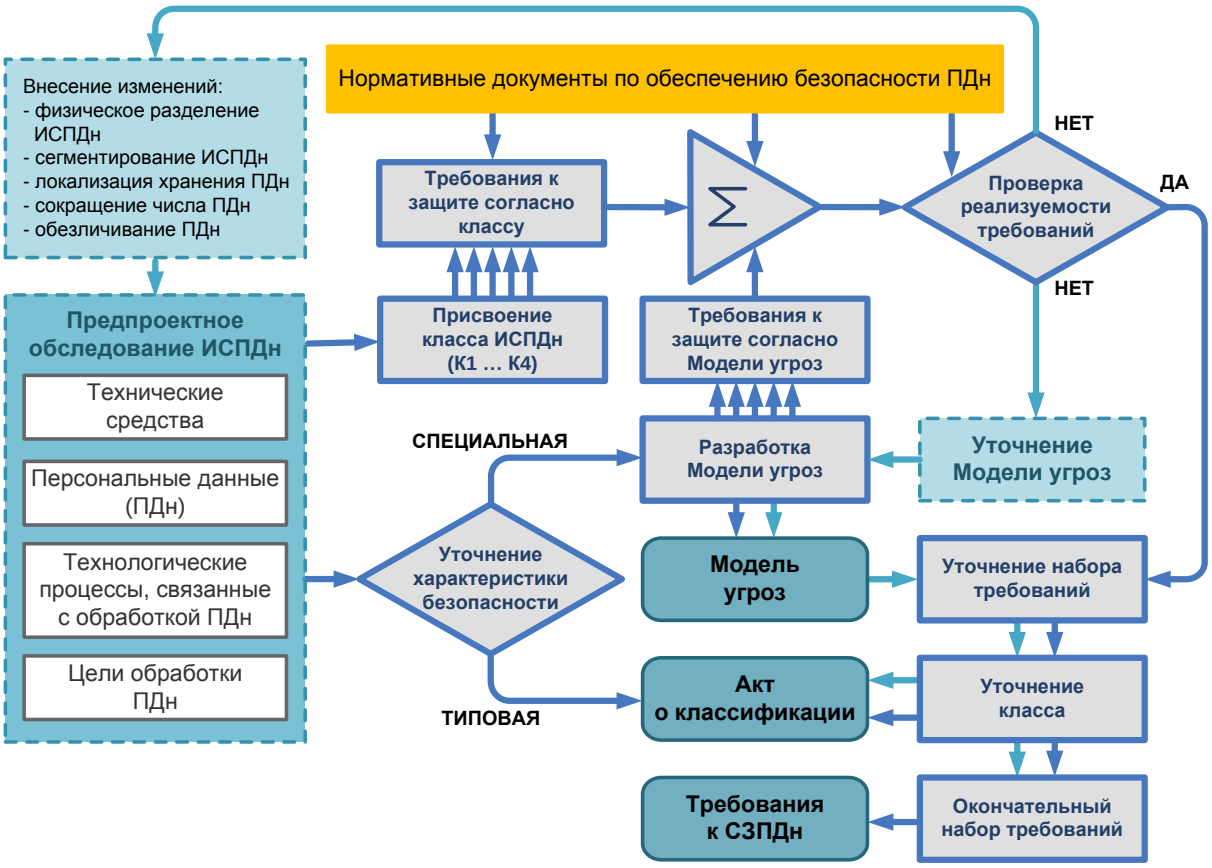


Рис. № 1

Для ИСПДн, идентифицированных как **типовые**, на этом, как правило, анализ заканчивается, и можно приступать к разработке требований к защите согласно классу и проверке их реализуемости. На результаты проверки могут повлиять технические особенности той или иной ИСПДн, наличие или отсутствие подходящего набора сертифицированных средств защиты, требования неизменности реализуемых бизнес-процессов, финансовые возможности организации-оператора и прочие факторы.

В случае положительного результата проверки реализуемости требований к системе защиты принимается окончательное решение о присвоении класса данной ИСПДн, составляется и утверждается Акт классификации и формулируется набор требований к системе защиты.

Основой для разработки требований к защите является методический документ ФСТЭК России «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных». При этом, как и в традиционной системе базовых принципов и

подходов к построению систем защиты, основанной на руководящем документе «Автоматизированные системы. Классификация автоматизированных систем и требования по защите информации» (Гостехкомиссия России, 1992 г.), определяющими являются:

- класс ИСПДн (К1, К2, К3, К4);
- структура ИСПДн (автономная, локальная, распределённая);
- наличие или отсутствие подключения к сетям общего пользования;
- режим обработки (однопользовательский или многопользовательский);
- наличие или отсутствие разграничения прав доступа.

В случае отрицательного результата проверки реализуемости требований к защите для какой-либо из ИСПДн для неё включаются процедуры внесения изменений (физического либо логического разделения, обезличивания ПДн и т.п.), после чего алгоритм идентификации и классификации ИСПДн запускается с исходной точки. Внесение изменений и проверка реализуемости требований повторяется до тех пор, пока не будет получен положительный результат оценки.

Для каждой ИСПДн, идентифицированной как **специальная**, по результатам предпроектного обследования проводится тот же комплекс процедур классификации, что и для типовых ИСПДн. Однако одновременно с формулировкой требований к защите, разработанным согласно определённому для неё классу, разрабатывается Модель угроз и дополнительный набор требований к защите согласно Модели угроз (о разработке моделей угроз читайте в разделе 7 настоящего документа).

Требования к защите, определённые для специальной ИСПДн согласно Модели угроз, сопоставляются и суммируются с требованиями, определёнными для неё согласно её классу (К1, К2, К3 или К4). При сопоставлении однотипных требований в качестве окончательного требования выбирается более жёсткое.

Итоговый набор требований проходит проверку их реализуемости так же, как это описано выше для типовых ИСПДн. Особенностью специальных ИСПДн является то, что в случае отрицательного результата проверки могут быть вместе либо по отдельности включены механизмы:

- доведения ИСПДн до состояния, в котором предъявляемый к ней набор требований будет полностью реализуем (прежде всего, механизмы корректировки инфраструктуры сети, описанные выше). Данные механизмы включаются и применяются один за другим либо в комплексе, и в итоге должны привести к положительному результату оценки реализуемости требований к СЗПДн;
- введения ограничений в модели угроз. Данный метод может потребовать как проведения серии специальных измерений и расчетов, так и согласования получаемых моделей угроз с регулирующими органами. Его целесообразно применять в том случае, если механизмы корректировки ИСПДн не привели к ожидаемому результату.

При наличии положительного результата оценки реализуемости требований к системе защиты конкретной специальной ИСПДн разработанная для неё Модель угроз принимается как окончательная, составляется и представляется на утверждение Акт классификации и формулируются в виде отдельного документа требования к защите.

Таким образом, в результате обработки результатов предпроектного обследования и реализации алгоритмов идентификации и классификации ИСПДн организация-оператор получает первый набор обязательных для разработки документов.

Ссылки

- 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»;
- Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России), Федеральной службы безопасности Российской Федерации (ФСБ России), Министерства информационных технологий и связи Российской Федерации (Мининформсвязи России) от 13 февраля 2008 г. № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных»;
- Методический документ «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных», ФСТЭК России, 15 февраля 2008 г. (пометка «для служебного пользования» снята решением ФСТЭК России от 16 ноября 2009 г.);
- Методический документ «Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», ФСТЭК России, 15 февраля 2008 г. (пометка «для служебного пользования» снята решением ФСТЭК России от 16 ноября 2009 г.);
- Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации. ФСБ России, 21 февраля 2008 г, № 149/5-144.

Шаг 7.
Разработать модель угроз для ИСПДн

Введение

Оценка актуальности угроз безопасности ПДн является ключевым элементом в процессе построения и управления СЗПДн. Корректное определение совокупности объектов негативного воздействия, присущих им уязвимостей, способов реализации этих уязвимостей и, как следствие, источников данного негативного воздействия позволяет дать качественную характеристику меры риска осуществления той или иной угрозы безопасности ПДн. В свою очередь, наличие формализованного описания актуальных угроз безопасности ПДн дает возможность подразделениям организаций и лицам, ответственным за безопасность ПДн:

- адекватно оценить необходимость реализации тех или иных мероприятий по обеспечению безопасности ПДн исходя из состояния защищённости ИСПДн на текущий момент;
- спрогнозировать развитие СЗПДн на краткосрочную и среднесрочную перспективу, провести оптимизацию бюджетов соответствующих подразделений, выставить приоритеты принимаемым мерам по обеспечению безопасности ПДн.

Российская практика создания СЗПДн показывает, что оценка актуальности угроз безопасности ПДн проводится при моделировании действий различных групп нарушителей, использующих те или иные уязвимости, характерные для анализируемой ИСПДн. Этот шаг осуществляется после выделения, обследования и классификации ИСПДн (см. Шаг 6) и предшествует проектированию и реализации СЗПДн (см. Шаг 8). В частности, основываясь на результатах моделирования актуальных угроз безопасности ПДн, формируются требования технического задания на СЗПДн. Результаты моделирования оформляются в документ «Модель угроз безопасности персональных данных при их обработке в ИСПДн».

Цели проведения работ

Целями данного шага являются определение актуальных угроз безопасности ПДн при их обработке в ИСПДн и составление модели угроз для каждой специальной ИСПДн, выделенной в ИТ-инфраструктуре организации-оператора.

Основание проведения работ

Согласно «Положению об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утверждённому постановлением Правительства Российской Федерации от 17 ноября 2007 г. № 781, п. 12, мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя «определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз…».

Кроме того, согласно п. 3.6 методического документа ФСТЭК Росси «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных», на предпроектной стадии по обследованию ИСПДн определяются (уточняются) угрозы безопасности ПДн применительно к конкретным условиям функционирования ИСПДн (разработка частной модели угроз).

А методический документ ФСТЭК Росси «Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (раздел 3) содержит прямое требование:

> *«Применительно к специальным информационным системам после определения класса системы оператором должна быть разработана модель угроз безопасности персональных данных ...».*

Выполняемые работы

В общем случае, работы по моделированию и определению актуальности угроз безопасности ПДн при их обработке в ИСПДн можно разделить на следующие этапы:

Определение общего перечня угроз безопасности ПДн

Угрозы безопасности ПДн при их обработке в ИСПДн представляются в виде совокупности возможных источников угроз НСД, уязвимостей программного и аппаратного обеспечения ИСПДн, способов реализации угроз, объектов воздействия (носителей защищаемой информации, директориев, каталогов, файлов с ПДн или самих ПДн) и возможных деструктивных воздействий.

Определение уровня исходной защищённости ИСПДн

По результатам анализа предоставленных исходных данных и результатов обследования состояния защищённости ИСПДн определяется уровень её исходной защищённости, характеризуемый числовым коэффициентом.

Под уровнем исходной защищённости ИСПДн понимается обобщённый показатель, зависящий от технических и эксплуатационных характеристик ИСПДн, который определяется на основании алгоритма, изложенного в методическом документе ФСТЭК России «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных».

Расчёт актуальности полученных угроз безопасности ПДн для анализируемой ИСПДн

На данном этапе проводится экспертная оценка сформированных наборов угроз безопасности ПДн с точки зрения частоты (вероятности) их реализации с определением для каждой угрозы соответствующего числового коэффициента с последующей вербальной интерпретацией полученных коэффициентов для всех выявленных угроз в диапазоне «низкая – средняя – высокая – очень высокая».

Под частотой (вероятностью) реализации угрозы в данном случае понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным

является реализация конкретной угрозы безопасности ПДн для данной ИСПДн в складывающихся условиях обстановки.

Далее оценивается опасность каждой угрозы. При оценке опасности на основе опроса экспертов в области компетенции Заказчика и экспертов в области защиты информации определяется вербальный показатель опасности угрозы по отношению к рассматриваемой ИСПДн.

После определения вышеназванных параметров из общего перечня угроз осуществляется выборка актуальных для ИСПДн угроз в соответствии с правилами, приведёнными в методическом документе ФСТЭК России «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных».

Создание документа «Модель угроз безопасности персональных данных при их обработке в ИСПДн»

Результаты вышеперечисленных работ отражаются в документе «Модель угроз безопасности персональных данных при их обработке в ИСПДн», который должен содержать следующую информацию:

- описание объекта моделирования (анализируемой ИСПДн) и его характеристик;
- перечни характерных для данной ИСПДн источников угроз безопасности персональных данных, уязвимостей компонентов ИСПДн, способов реализации данных уязвимостей в рамках анализируемой ИСПДн, объектов воздействия и последствий реализации вышеуказанных способов;
- перечни характерных для данной ИСПДн угроз безопасности ПДн;
- оценку ущерба (опасности) для субъектов персональных данных от реализации тех или иных угроз безопасности ПДн;
- анализ рисков реализации вышеуказанных угроз;
- выводы относительно класса криптосредств, обязательных к использованию в анализируемой ИСПДн.

Результат

В результате проведенных работ для каждой идентифицированной и классифицированной ИСПДн должен быть сформирован документ «Модель угроз безопасности ПДн при их обработке в ИСПДн», составленный с учётом методических рекомендаций ФСТЭК России, а при использовании криптографических средств – также методических рекомендаций ФСБ России.

Ограничения / на что стоит обратить внимание

Как и любой этап построения системы защиты персональных данных, процесс создания модели угроз безопасности ПДн не лишен трудностей. Среди основных рисков данного этапа можно выделить следующие:

- корректность определения элементов описания угроз, характерных для анализируемой ИСПДн;
- корректность определения вероятности реализации угрозы;
- корректность определения ущерба (опасности) для субъекта персональных данных от реализации угроз безопасности ПДн.

Необходимо также учесть следующие рекомендации, специально разработанные ФСБ России для случая, когда для обеспечения безопасности ПДн используются СКЗИ (см. методический документ «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», п. 2.4):

> *В случае обеспечения безопасности персональных данных без использования криптосредств при формировании модели угроз используются методические документы ФСТЭК России.*
>
> *В случае определения оператором необходимости обеспечения безопасности персональных данных с использованием криптосредств при формировании модели угроз используются методические документы ФСТЭК России и настоящие Методические рекомендации. При этом из двух содержащихся в документах ФСТЭК России и Методических рекомендациях однотипных угроз выбирается более опасное.*
>
> *По согласованию с ФСТЭК России и ФСБ России допускается формирование модели угроз только на основании настоящих Методических рекомендаций.*
>
> *При обеспечении безопасности персональных данных, при обработке в информационных системах, отнесенных к компетенции ФСБ России, модели угроз формируется только на основании настоящих Методических рекомендаций.*

Ссылки

При разработке модели угроз рекомендуется воспользоваться следующими материалами:

- 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»;
- Методический документ «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных», ФСТЭК России, 15 февраля 2008 г. (пометка «для служебного пользования» снята решением ФСТЭК России от 16 ноября 2009 г.);
- Методический документ «Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», ФСТЭК России, 15 февраля 2008 г. (пометка «для служебного пользования» снята решением ФСТЭК России от 16 ноября 2009 г.);
- Методический документ «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», ФСТЭК России, 15 февраля 2008 г. (для служебного пользования»);
- Методический документ «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», ФСТЭК России, 14 февраля 2008 г. (пометка «для служебного пользования» снята решением ФСТЭК России от 16 ноября 2009 г.);

- 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 февраля 2008 г. № 149/54-144);
- 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 февраля 2008 г. № 149/6/6-622);
- ГОСТ Р ИСО/МЭК 13335-3-2007 «Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий»;
- ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».

Шаг 8.
Спроектировать и реализовать систему защиты персональных данных

Введение

Создание СЗПДн является неотъемлемой частью реализации всего спектра требований, предъявляемых к оператору ПДн федеральным законом № 152-ФЗ и соответствующими подзаконными актами. Субъекты персональных данных, передавая свои сведения оператору, вправе рассчитывать на то, что безопасность этих сведений будет обеспечена всеми необходимыми мерами со стороны оператора. Это подразумевает под собой не только использование технических средств защиты, но и проведение определённых организационных мероприятий, направленных на обеспечение безопасности ПДн, обрабатываемых в каждой конкретной ИСПДн, эксплуатируемой оператором.

Цели проведения работ

Целями выполняемых работ являются разработка и создание для каждой ИСПДн системы защиты персональных данных, соответствующей законодательству Российской Федерации, лучшим мировым практикам в области обеспечения ИБ и отвечающей требованиям, предъявляемым методическими документами ФСТЭК России и ФСБ России к соответствующему классу ИСПДн.

Основание проведения работ

Согласно «Положению об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утверждённому постановлением Правительства Российской Федерации от 17 ноября 2007 г. № 781, п. 2:

> *«Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии».*

Согласно методическому документу ФСТЭК России «Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», раздел 4:

> *«Обеспечение безопасности ПДн при их обработке в автоматизированных ИСПДн должно проводиться путем выполнения комплекса организационных и технических мероприятий (применения технических средств), в рамках системы*

(подсистемы) защиты персональных данных, развертываемой в ИСПДн в процессе её создания или модернизации».

Выполняемые работы

Разработка и создание СЗПДн является нетривиальной научно-практической задачей, сложность которой адекватно соответствует сложности структуры и характеристикам ИСПДн как объекта внедрения.

Предлагается следующее структурное представление основных стадий создания СЗПДн.

Организация проведения работ по защите ПДн

Основой для организации работ по построению СЗПДн в каждой крупной организации-операторе служит **концепция информационной безопасности или замысел защиты.** Данный документ является высокоуровневым, в нём руководство заявляет о наличии в организации и проводит анализ производственной сферы, связанной с использованием информации ограниченного распространения (персональных данных), подлежащей защите в соответствии с требованиями федерального законодательства, делает вывод о необходимости выполнять требования к безопасности такой информации. Данный документ определяет нормативно-правовое обеспечение, цели, задачи и основные принципы создания системы обеспечения безопасности ПДн, содержание базовых компонентов СЗПДн и основные направления их формирования и развития.

Концепция служит основой для формирования программы и практического плана действий организации-оператора по приведению процессов, связанных с обработкой информации ограниченного распространения (персональных данных), в соответствие с требованиями федерального законодательства и нормативно-правовыми актами федеральных органов исполнительной власти.

Следующим звеном в проведении работ по защите ПДн является разработка и введение мер, которые необходимо применять при защите информации ограниченного доступа, а также определение порядка работ по построению СЗПДн для каждой конкретной ИСПДн, идентифицированной и описанной в структуре организации. Требуется учесть не только технические, но и организационные аспекты защиты информации, будь то пропускной режим на территорию организации, допуск персонала в помещения и к техническим средствам ИСПДн, персональная ответственность лиц, занимающихся обработкой ПДн в организации, или физическая защита её ресурсов.

Разработка требований по обеспечению безопасности ПДн при обработке в ИСПДн

Для каждой из ИСПДн, используемых в организации, с учётом их класса, обрабатываемых персональных данных, особенностей и условий функционирования выполняется разработка требований по обеспечению безопасности ПДн при обработке в ИСПДн, определяющих необходимые для реализации меры обеспечения безопасности. Данные требования являются основой для разработки технического задания, выбора средств защиты и технического проектирования.

В соответствии с вышеописанным алгоритмом классификации ИСПДн (см. Шаг 6), разработка требований к системе защиты и проверка их реализуемости в каждой из ИСПДн, для которой они были разработаны, является неотъемлемой частью процесса выделения и классификации ИСПДн. Она может считаться успешной лишь в том случае,

когда все наборы требований для всех ИСПДн признаны реализуемыми для данной организации-оператора.

Разработка технического задания

Следующим этапом создания СЗПДн является разработка технического задания, определяющего требования к проведению работ по созданию СЗПДн и содержащего следующие разделы:

- обоснование разработки СЗПДн;
- исходные данные создаваемой (модернизируемой) ИСПДн в техническом, программном, информационном и организационном аспектах;
- класс ИСПДн;
- ссылку на нормативные документы, с учётом которых будет разрабатываться СЗПДн и приниматься в эксплуатацию ИСПДн;
- конкретизацию мероприятий и требований к СЗПДн;
- перечень предполагаемых к использованию сертифицированных средств защиты информации;
- обоснование проведения разработок собственных средств защиты информации при невозможности или нецелесообразности использования имеющихся на рынке сертифицированных средств защиты информации;
- состав, содержание и сроки проведения работ по этапам разработки и внедрения СЗПДн.

Проектирование СЗПДн

Следующим после разработки технического задания этапом является проектирование СЗПДн, включающее в себя выбор необходимых для внедрения средств и мер защиты персональных данных.

При этом следует учитывать, что для защиты ИСПДн от угроз несанкционированного доступа должны применяться средства защиты информации, имеющие сертификаты ФСБ России и ФСТЭК России, список которых можно найти на официальных сайтах.

Система защиты в типовом варианте представляет собой совокупность следующих подсистем:

- управления доступом;
- регистрации и учёта;
- обеспечения целостности;
- криптографической защиты;
- антивирусной защиты;
- обнаружения вторжений.

Выбор средств защиты информации при проектировании необходимо осуществлять с учётом того, что итоговый набор реализуемых мер защиты должен удовлетворять требованиям, предъявляемым к ИСПДн соответствующего класса, концентрированное выражение которых приведено в методическом документе ФСТЭК России «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных».

При этом необходимо обеспечить выполнение следующих общих требований и условий:

- для построения подсистемы антивирусной защиты в средствах вычислительной техники необходимо применять сертифицированные средства антивирусной защиты;
- при подключении ИСПДн к сетям общего пользования необходимо обеспечить межсетевое экранирование, применяя при этом аппаратные, программные или аппаратно-программные межсетевые экраны, имеющие сертификат соответствия по классу защищённости не ниже, чем предъявляется в требованиях;
- во всех средствах вычислительной техники – как в серверах, так и в пользовательских, – необходимо обеспечить защиту от НСД и обеспечить регистрацию и верифицированный учёт пользователей.

Кроме того, для защиты ИСПДн 1-го и 2-го классов от утечки по каналам побочных электромагнитных излучений и наводок (ПЭМИН) помимо использования серийно выпускаемых сертифицированных СЗИ необходимо обеспечить ряд следующих мер:

- размещение понижающих трансформаторных подстанций электропитания и контуров заземления на территории контролируемой зоны;
- обеспечение развязки цепей электропитания объектов защиты с помощью защитных фильтров, блокирующих информативный сигнал;
- обеспечение электромагнитной развязки между линиями связи и другими цепями вспомогательных технических средств и систем, выходящими за пределы КЗ, и информационными цепями, по которым циркулирует защищаемая информация.

А в том случае, когда в ИСПДн предусмотрены функции голосового ввода ПДн либо воспроизведение информации акустическими средствами ИСПДн, то для ИСПДн 1-го класса должны быть реализованы мероприятия по защите от перехвата такой информации за счёт использования сертифицированных СЗИ.

Результаты проектирования оформляются в виде пакета проектной документации в соответствии с системой государственных стандартов Российской Федерации «Единая система конструкторской документации» и стандартами серии «Информационная технология. Комплекс стандартов на автоматизированные системы».

Внедрение и контроль

Внедрение разработанных при проектировании ИСПДн технических решений осуществляется в соответствии с технической документацией на внедряемые средства и системы. При этом особое внимание требуется уделять корректной настройке всех механизмов, обеспечивающих соответствие реализованного функционала СЗПДн разработанному для неё набору требований по обеспечению безопасности ПДн при обработке в ИСПДн.

По окончании внедрения средств защиты проводится итоговый контроль защищённости.

Контроль защищённости информации от НСД проводится с помощью сертифицированных сканеров уязвимостей.

Контроль защищённости информации от утечек за счёт побочных электромагнитных излучений и наводок, а также контроль акустической защищённости проводится с применением специальных сертифицированных приборов контроля и с использованием соответствующих программ и методик.

Разработка документации

Ввод СЗПДн в эксплуатацию предполагает собой не только внедрение технических средств, но и разработку пакета организационной и методической документации, позволяющей эффективно оценивать и контролировать состояние защищённости ИСПДн.

Инструкции – документы, содержащие детализированные требования по одному из аспектов обеспечения безопасности ПДн для поддержания СЗПДн в актуальном состоянии. Часть инструкций разрабатывается в случае, если внедрение технических средств невозможно, и необходимо принимать организационные мероприятия в части защиты ПДн.

Регламенты – документы, описывающие пошаговый порядок обработки информации, содержащей персональные данные. В части регламентов стоит учесть взаимодействие организации и её контрагентов между собой и описать чёткие правила и порядок передачи информации, содержащей персональные данные.

Журналы – рабочие документы, необходимые как средство контроля выполнения персоналом требований по обеспечению безопасности персональных данных. Они предъявляются регулятору при проверке для демонстрации того, что мероприятия по защите персональных данных организацией-оператором проводятся с определённой периодичностью.

Особое место стоит уделить таким видам организационных мероприятий, как инструктаж пользователей в части защиты ПДн. Данные мероприятия необходимо учитывать в особом журнале под росписью каждого проинструктированного лица, допущенного к обработке ПДн, а также занимающегося обслуживанием ИСПДн.

Результат

Результатом выполнения описанных работ является комплексная система защиты персональных данных в организации, соответствующая требованиям федерального законодательства и нормативно-правовым актам в области информационной безопасности:

- обеспечивающая выполнение требований к безопасности ПДн при их обработке в ИСПДн данного класса;
- сформированная как совокупность мероприятий, осуществляемых на всех стадиях жизненного цикла ИСПДн, согласованных по цели, задачам, месту и времени;
- направленная на предотвращение (нейтрализацию) и парирование угроз безопасности ПДн в ИСПДн, восстановление нормального функционирования ИСПДн после нейтрализации угрозы, минимизацию как непосредственного, так и опосредованного ущерба от возможной реализации таких угроз.

Ограничения / на что стоит обратить внимание

Необходимо обратить внимание на выбор средств защиты информации. В реестрах сертификатов ФСТЭК России и ФСБ России указывается, выдан ли сертификат на всю

серию или на единичный экземпляр, приводятся сведения об ограничениях и о возможности применения данного СЗИ в ИСПДн определённого класса.

Использование только СЗИ от НСД не является достаточным для защиты ИСПДн. В ряде случаев, определённых методическими документами ФСТЭК России и ФСБ России, требуется применение средств межсетевого экранирования, обнаружения вторжений, криптографической защиты и др. Возможна сертификация ранее внедрённых в систему СЗИ, если установка имеющихся сертифицированных СЗИ трудоёмка или нецелесообразна.

Разработка внутренних организационно-распорядительных документов по обеспечению безопасности ПДн должна исключать возможность «обхода» принятых требований либо их осознанного игнорирования в силу банальной нереализуемости в условиях бизнеса и рынка.

Различные внутренние службы и подразделения могут не принять документы по защите информации или препятствовать их подписанию в случае, когда эти службы не были задействованы на этапе разработки данной документации. Созданная система организационных мер нуждается в постоянной поддержке и актуализации. В противном случае она в достаточно короткое время перестает учитывать существующие реалии бизнеса, что приведет к игнорированию требований документов со стороны сотрудников. Мероприятия по ознакомлению сотрудников с принятыми требованиями и повышение их осведомленности в вопросах обеспечения информационной безопасности должны проводиться регулярно и в отношении всего персонала.

Ссылки

- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- 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»;
- BS 10012:2009 Data protection – Specification for a personal information management system;
- ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»;
- ГОСТ Р ИСО/МЭК 19011—2003 Руководящие указания по аудиту систем менеджмента качества и/или систем экологического менеджмента;
- Методический документ «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных», ФСТЭК России, 15 февраля 2008 г. (пометка «для служебного пользования» снята решением ФСТЭК России от 16 ноября 2009 г.);
- Методический документ «Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», ФСТЭК России, 15 февраля 2008 г. (пометка «для служебного пользования» снята решением ФСТЭК России от 16 ноября 2009 г.);
- Указ Президента Российской Федерации № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» от 17 марта 2008 г.;

- Руководящий документ «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)». Утверждён приказом Гостехкомиссии России от 30 августа 2002 г. № 282 (для служебного пользования).

Шаг 9.
Провести аттестацию ИСПДн по требованиям безопасности или продекларировать соответствие

Введение

Аттестация и декларирование соответствия – различные варианты оценки соответствия требованиям безопасности информации, применяемые к ИСПДн как к защищаемым объектам информатизации. Оценка соответствия является обязательной процедурой, завершающей этап ввода в строй ИСПДн с внедрённой в неё системой защиты.

Аттестация – комплекс организационно-технических мероприятий, в результате которых подтверждается, что объект информатизации соответствует требованиям стандартов или иных нормативных документов по безопасности информации. Аттестация применяется по отношению к ИСПДн 1 и 2 классов.

Декларирование соответствия – форма подтверждения соответствия продукции требованиям технических регламентов (федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании»). Применительно к ИСПДн декларирование соответствия означает подтверждение соответствия ИСПДн требованиям к безопасности обрабатываемых в ней персональных данных. Декларирование соответствия применяется по отношению к ИСПДн 3 класса, а по решению оператора – и к ИСПДн 4 класса.

Цель проведения работ

Целями выполняемых работ являются подтверждение работоспособности информационной системы организации с внедрёнными в её инфраструктуру средствами и системами защиты ПДн и подтверждение соответствия каждой идентифицированной ИСПДн требованиям к безопасности информации, предъявляемым согласно присвоенному ей классу и принятой модели угроз, с получением документа, удостоверяющего соответствие.

Основание проведения работ

Аттестация является обязательной процедурой при оценке соответствия всех объектов информатизации, на которых предусмотрена обработка информации ограниченного распространения, подлежащей защите в соответствии с требованиями федерального законодательства, и в том числе, как было отмечено выше, ИСПДн 1 и 2 класса.

Аттестация информационных систем предполагает проверку не отдельных компонентов, а законченной информационной системы, что является сложной комплексной задачей. Защищённость информационной системы зависит от многих факторов — аппаратного обеспечения, программного обеспечения, различий в отдельных компонентах сборки, регламентов функционирования. Для успешной аттестации законченной информационной системы необходимо доверие ко всем компонентам, из которых она состоит.

Порядок аттестации определяется Положением по аттестации объектов информатизации по требованиям безопасности информации (Гостехкомиссия России, 1994 г.) и проводится

в соответствии с традиционными методами и подходами, описанными в руководящих документах Гостехкомиссии России 1992 – 2002 годов.

Правовое поле декларирования соответствия ограничено федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании». Технические регламенты, а также официальные рекомендации ФСТЭК России и ФСБ России, описывающие процедуры декларирования соответствия, до настоящего времени не приняты, терминология и методология процедуры декларирования в руководящих и методических документах по защите ПДн не проработаны. В связи с этим оценка соответствия методом декларирования проводится по тем же нормам и методикам, что и аттестация. Различие заключается лишь в том, что декларирование соответствия и оформление Декларации соответствия ИСПДн требованиям по защите информации оператор, при наличии необходимого инструментария и квалифицированного персонала, проводит самостоятельно, тогда как аттестацию ИСПДн может проводить только организация, имеющая лицензию ФСТЭК России на деятельность в области технической защиты конфиденциальной информации.

По состоянию на 1 января 2010 г. каких бы то ни было документов, специально определяющих порядок оценки соответствия (аттестации, декларирования) объектов информатизации, предназначенных для обработки информации конфиденциального характера (персональных данных), не составляющей государственную тайну, учитывающих особенности данных систем и более низкий уровень требований по сравнению с защитой государственной тайны, в правовом поле Российской Федерации не существует.

Выполняемые работы

В соответствии с «Положением по аттестации…», в ходе аттестационных испытаний (а применительно к ИСПДн 3 класса – при разработке Декларации соответствия) для каждой идентифицированной ИСПДн как для защищаемого объекта выполняются следующие виды работ:

- анализ организационной структуры ИСПДн, информационных потоков, состава и структуры комплекса технических средств и программного обеспечения, системы защиты информации на объекте, разработанной документации и её соответствия установленным требованиям;
- проверка правильности классификации ИСПДн, выбора и применения средств и систем защиты информации;
- при необходимости, сертификационные испытания несертифицированных СЗИ на аттестуемом объекте или анализ результатов их испытаний в испытательных центрах (лабораториях) по сертификации;
- проверка уровня подготовки кадров и распределения ответственности персонала за обеспечение выполнения требований по безопасности информации;
- комплексные испытания СЗПДн в реальных условиях эксплуатации путем проверки фактического выполнения установленных требований на различных этапах технологического процесса обработки персональных данных;
- оформление протоколов испытаний и заключений по результатам оценки соответствия с конкретными рекомендациями по устранению допущенных нарушений и приведению СЗПДн в соответствие с установленными требованиями.

При успешном результате аттестационных испытаний на подвергнутый испытаниям объект – ИСПДн выдаётся документ, удостоверяющий соответствие: «Аттестат соответствия» либо «Декларация соответствия».

При несоответствии объекта требованиям по безопасности информации и невозможности оперативно устранить отмеченные недостатки принимается решение об отказе в выдаче документа, удостоверяющего соответствие.

При наличии замечаний непринципиального характера документ, удостоверяющий соответствие, может быть выдан после проверки устранения этих замечаний.

Дальнейшая эксплуатация объекта информатизации осуществляется в полном соответствии с аттестатом (декларацией), утверждённой организационно-распорядительной и эксплуатационной документацией, с учётом соответствующих требований руководящих и методических документов ФСТЭК России и ФСБ России.

Результат

Результатом шага являются комплекты документов на каждую идентифицированную ИСПДн, содержащие:

- материалы испытаний (акты установки средств защиты, протоколы, заключения);
- Аттестаты соответствия требованиям безопасности информации (для ИСПДн классов К1 и К2);
- Декларации соответствия (для ИСПДн класса К3).

Ограничения / на что стоит обратить внимание

Нечёткое понимание операторами некоторых положений нормативно-правовых актов в области оценки соответствия ИСПДн требованиям безопасности информации может привести к неточностям в организационно-распорядительной документации и ошибкам в системе управления информационной безопасностью, ведущим к наложению запрета на обработку ПДн в ИСПДн.

Чтобы избежать недоразумений, предлагается запомнить и использовать несколько правил.

Правило первое. Целью всех процессов, включающих в себя элементы оценки соответствия, является обеспечение необходимого уровня защищённости конкретного объекта информатизации (защищённого помещения, персонального компьютера, локальной вычислительной сети), то есть создание объекта, на который может быть выдан документ, посредством которого подтверждается наличие на объекте необходимых и достаточных условий, обеспечивающих выполнение установленных требований руководящих документов по защите информации.

Итак, во главе угла – ИСПДн как объект и аттестат (декларация) на этот объект.

Правило второе. Согласно требованиям нормативно-правовых актов в области обеспечения безопасности информации, для защиты информации ограниченного распространения следует применять исключительно сертифицированные СЗИ. Если по результатам предварительных испытаний делается вывод о необходимости применения

специальных средств защиты конфиденциальной информации (персональных данных), следует выбирать только те СЗИ, на которые уполномоченными на то органами (ФСТЭК России и ФСБ России) выдан и имеется действующий сертификат.

Принципиально возможен такой вариант, когда в ИСПДн изначально используются несертифицированные СЗИ, и организовывается сертификация ИСПДн в целом и её последующая аттестация. Однако, это является длительным и дорогостоящим процессом. Кроме того, состояние всей системы после аттестации жестко фиксируется. Это означает, что при внесении в систему любых изменений — от перенастройки до установки обновлений ПО — потребуется её повторная сертификация и аттестация.

Сертификат рекомендуется иметь в виду не как документ, относящийся к объекту в целом, а как относящийся лишь к одному из средств его защиты.

Правило третье и главное. Нельзя проводить закрытые мероприятия с обсуждением конфиденциальной информации (голосовой ввод ПДн) в помещениях или обрабатывать конфиденциальную информацию (персональные данные) на компьютерах (в ИСПДн), на которые не выданы аттестаты соответствия требованиям безопасности информации или соответствие которых установленным требованиям не подтверждено оформленной должным образом декларацией соответствия.

Невыполнение данного условия является грубейшей формой нарушения закона и чревато самыми серьёзными последствиями для оператора.

Ссылки

- Положение по аттестации объектов информатизации по требованиям безопасности информации, утверждённое Председателем Гостехкомиссии России 25 ноября 1994 г.;
- Руководящие документы по защите информации от несанкционированного доступа, Гостехкомиссия России, 1992 – 1997 г.г.;
- Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании»;
- Руководящий документ «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)». Утверждён приказом Гостехкомиссии России от 30 августа 2002 г. № 282 (для служебного пользования);
- Сборник временных методик оценки защищённости конфиденциальной информации от утечки по техническим каналам, утверждённых первым заместителем Председателя Гостехкомиссии России 8 ноября 2001 г.;
- Методический документ «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных», ФСТЭК России, 15 февраля 2008 г. (пометка «для служебного пользования» снята решением ФСТЭК России от 16 ноября 2009 г.);
- Методический документ «Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», ФСТЭК России, 15 февраля 2008 г. (пометка «для служебного пользования» снята решением ФСТЭК России от 16 ноября 2009 г.);
- 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. ФСБ России, 21 февраля 2008 г., № 149/6/6-622;
- Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации. ФСБ России, 21 февраля 2008 г, № 149/5-144.

Шаг 10.
Определить перечень мер по защите ПДн, обрабатываемых без использования средств автоматизации

Введение

Законом «О персональных данных» определяется, что обработка персональных данных может вестись как с использованием средств автоматизации (автоматизированная обработка), так и без использования таковых (неавтоматизированная обработка). При этом необходимость осуществления неавтоматизированной обработки ПДн может быть обусловлена как потребностями бизнеса, так и необходимостью минимизации рисков ИБ, связанных с использованием средств автоматизации. Как минимум, к преимуществам неавтоматизированной обработки можно отнести следующее:

- отсутствие необходимости подачи уведомления об обработке персональных данных в уполномоченный орган по защите прав субъектов персональных данных;
- простота реализации требований нормативно-правовых актов;
- существенное снижение затрат на построение системы защиты информации, в частности затрат на технические средства обработки ПДн и технические средства защиты.

Есть у такой обработки и безусловные недостатки, связанные с невысокой производительностью выполнения операций с использованием бумажных носителей.

Цель проведения работ

Целью выполнения работ на данном шаге является построение эффективного и работоспособного порядка обращения с персональными данными, обрабатываемыми без использования средств автоматизации, и создание условий, обеспечивающих безопасность ПДн при неавтоматизированной обработке.

Основание проведения работ

Согласно «Положению об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утверждённому постановлением Правительства Российской Федерации от 15 сентября 2008 г. №, правила обработки персональных данных, осуществляемой без использования средств автоматизации, должны применяться с учётом требований данного Положения.

Указанное Положение определяет как особенности организации обработки ПДн, осуществляемой без использования средств автоматизации, так и меры по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации.

Кроме того, методическим документом ФСТЭК России «Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах

персональных данных» рекомендовано использование традиционных подходов к технической защите информации в автоматизированных системах. В связи с этим необходимо в максимально полной мере в этой работе использовать также рекомендации руководящего документа Гостехкомиссии России «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)». В данном руководящем документе сформирован ряд требований организационно-режимного характера, составляющие основу современных требований по обеспечению безопасности персональных данных, в том числе обрабатываемых без использования средств автоматизации.

Выполняемые работы

В целях обеспечения безопасности персональных данных при осуществлении их обработки без использования средств автоматизации, что в общем случае понимается как обработка ПДн, хранящихся на различных материальных носителях (бумага, магнитные ленты, микрофильмы и пр.), как правило, необходимо провести следующие мероприятия.

Провести инвентаризацию и определить места хранения носителей ПДн

Необходимо определить перечни ПДн (материальных носителей ПДн), обработка которых осуществляется без использования средств автоматизации, и для каждой категории таких ПДн определить места их хранения и установить перечень лиц, осуществляющих обработку ПДн либо имеющих к ним доступ.

Должно быть обеспечено размещение ПДн на материальных носителях таким образом, чтобы ПДн были обособлены от другой информации и имели идентичные цели их обработки, т.е. на одном материальном носителе не должно быть ПДн, обрабатываемых для различных целей.

Хранение материальных носителей ПДн должно быть организовано таким образом, чтобы:

- обеспечивалось раздельное хранение материальных носителей ПДн, обработка которых осуществляется в различных целях;
- обеспечивалась сохранность ПДн и исключался несанкционированный доступ к ним (перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются организацией-оператором).

Уведомить персонал

Все работники организации-оператора, допущенные к неавтоматизированной обработке ПДн, должны быть уведомлены под роспись:

- о факте обработки ими ПДн;
- о категориях обрабатываемых ПДн;
- об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами организации-оператора.

Разработать внутренние нормативные документы

Формы документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее – типовая форма), должны быть приведены в соответствие следующим требованиям:

- типовая форма или связанные с ней документы (инструкция по её заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;
- типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных (при необходимости наличия такого согласия);
- типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;
- типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

Принять меры по обеспечению безопасности ПДн

Несмотря на то, что меры по обеспечению безопасности материальных носителей ПДн для каждой организации-оператора индивидуальны и выбираются ею самостоятельно, следующие меры и средства рекомендуются как базовые:

- меры, обеспечивающие безопасное хранение материальных носителей ПДн. К таким мерам относятся закупка и установка сейфов, металлических шкафов, создание специально оборудованных помещений и т.п.;
- меры защиты от НСД к ПДн (материальным носителям ПДн). К таким мерам относятся установка замков, систем сигнализации и видеонаблюдения и т.п.;
- средства гарантированного уничтожения ПДн (материальных носителей ПДн). К таким относятся средства измельчения, сжигания, размагничивания и другие им подобные, гарантирующие невозможность последующего восстановления данных.

Результат

Реализация всех вышеперечисленных мер позволит организации-оператору привести в соответствие с законодательством РФ все процессы обработки ПДн, осуществляемой без использования средств автоматизации, и тем самым обеспечить:

- исключение обработки неучтенных и/или ненужных (избыточных) ПДн;
- исключение неумышленной или несанкционированной компрометации ПДН как при их обработке, так и после их уничтожения;

- защиту ПДн от непредвиденного уничтожения, в том числе при наступлении локальных катастроф (пожар, затопление и т.п.);
- повышенное доверие к себе как к оператору ПДн и в целом улучшение репутации;
- минимизацию рисков подпадания под санкции со стороны контролирующих органов.

Ограничения / на что стоит обратить внимание

При проведении работ по защите ПДн, обрабатываемых без использования средств автоматизации, необходимо уделить отдельное внимание созданию следующих условий, способствующих достижению целей работ на данном шаге:

- меры и средства защиты ПДн не должны оказывать негативного влияния на сроки и трудоемкость процессов обработки ПДн;
- процессы обработки ПДн (распространение, уничтожение, блокирование всех ПДн и/или какой-либо их части) должны быть оптимизированы и постоянно совершенствоваться;
- необходимо обязательное обучение сотрудников организации-оператора (особенно вновь принятых) и регулярное подтверждение соблюдения ими установленных требований по обеспечению безопасности ПДн;
- для соблюдения требований законодательства РФ и внутренних формализованных требований оператора по защите ПДн необходимо регулярное проведение контрольных мероприятий (аудит, мониторинг и т.п.);
- при выборе и реализации мероприятий по защите ПДн рекомендуется учитывать международные стандарты и лучшие практики в области информационной безопасности (ISO, BS, NIST).
- необходимо регулярно оценивать адекватность и достаточность принятых мер (и при необходимости их пересматривать) по обеспечению безопасности материальных носителей ПДн с учётом особенностей использования этих сведений в деятельности организации и возникающих при этом рисков.

Ссылки

- Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», раздел II;
- Руководящий документ «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)». Утверждён приказом Гостехкомиссии России от 30 августа 2002 г. № 282 (для служебного пользования), п.п. 5.1.3, 5.2.2, 5.2.7.

Шаг 11.
Обеспечить постоянный контроль защищённости ПДн

Введение

Построение системы защиты персональных данных в организации является сложным многоэтапным процессом, состоящим из следующих основных этапов: обследование, проектирование и внедрение, более подробно описанных в предыдущих шагах настоящего методического пособия. Распространённым случаем является то, что на этом организация-оператор останавливается, посчитав, что завершение проекта по созданию комплексной СЗПДн означает полное выполнение всех требований к безопасности. Однако это не так, поскольку кроме выполнения всех установленных требований необходимо ещё обеспечить и контроль их исполнения в ходе эксплуатации ИСПДн. Кроме того, для эффективного использования СЗПДн необходимо её постоянно совершенствовать исходя из результатов периодического анализа.

Цель проведения работ

Целью контроля за обеспечением уровня защищённости ПДн является проверка того, что процессы и системы обработки и защиты ПДн в организации:

- соответствуют требованиям, предъявляемым законодательством к защите и обработке персональных данных;
- эффективно реализованы и сопровождаются;
- выполняются в соответствии с ожиданиями, сформированными при проектировании и внедрении системы защиты персональных данных.

Основание проведения работ

Согласно «Положению об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утверждённому постановлением Правительства Российской Федерации от 17 ноября 2007 г. № 781, п. 11, при обработке ПДн в информационной системе должен быть обеспечен постоянный контроль за обеспечением уровня защищённости ПДн.

Выполняемые работы

Для того, чтобы достичь поставленных целей, следует регулярно (не реже одного раза в год) проводить в организации-операторе процедуры мониторинга и анализа управления и обеспечения безопасности персональных данных – внутренний аудит.

Аудит – это систематический, независимый и документированный процесс получения свидетельств аудита и объективного их оценивания с целью установления степени выполнения согласованных критериев аудита.

В рамках анализа и мониторинга СЗПДн такими критериями могут быть:

- требования регулирующих органов (федеральный закон от 27 июля 2007 г. № 152-ФЗ «О персональных данных», подзаконные акты, руководяще и методические документы ФСТЭК России и ФСБ России и др.);
- требования внутренних организационно-распорядительных документов (приказов, положений, регламентов, инструкций и др.) организации-оператора, регламентирующих обработку и защиту ПДн;
- требования корпоративных стандартов, технических заданий и проектов, а также эксплуатационной документации на системы и СЗИ;
- требования к СЗПДн, сформулированные по результатам обследования, классификации и разработки моделей угроз для ИСПДн;
- положения признанных на территории РФ международных стандартов и директив по защите ПДн;
- согласованные и документированные требования партнеров и/или клиентов.

Внутренний аудит проводится силами самой организации или от её имени сторонними компаниями, имеющими соответствующие права и опыт на осуществление данной деятельности.

Хорошей практикой для организаций является разработка и утверждение внутреннего документа организации, устанавливающего конкретные требования к процедурам контроля обеспечения безопасности ПДн. Данный документ должен быть в обязательном порядке согласован с положениями политики информационной безопасности организации-оператора.

Мероприятия по проведению аудита разделяются на следующие этапы.

Подготовка к аудиту – этап, в ходе которого формируется план аудита, содержащий область и критерии аудита исходя из ранее определённых целей. План аудита должен быть согласован с руководителем организации и доведен до проверяемых лиц.

Проведение аудита – этап сбора свидетельств аудита посредством анализа документации, интервьюирования сотрудников, сбора доказательств и непосредственного наблюдения за проверяемыми процессами и событиями. Все основные характеристики процессов сбора свидетельств аудита (время и длительность интервьюирования, средства и права доступа к данным и т.д.) должны быть заблаговременно определены и согласованы с проверяемыми лицами.

Анализ собранных свидетельств аудита – этап, в ходе которого осуществляется анализ собранных свидетельств аудита и их сравнение с критериями аудита. Все выявленные несоответствия свидетельств и критериев аудита должны быть отражены в отчёте об аудите.

Формирование отчёта об аудите – это завершающий этап аудита, на котором осуществляется консолидация и обобщенное формальное представление всех этапов аудита, выводов аудита и заключений по результатам аудита. Отчет об аудите должен быть

согласован с проверяемыми лицами. В случае невозможности согласования отчета об аудите в виду взаимного несогласия по каким-либо его положениям эти положения и причины несогласий должны быть отражены в акте разногласий.

Действия по результатам аудита – включают выполнение рекомендаций, содержащихся в выводах аудита. Для этого проверяемым лицом должен быть разработан, согласован с аудитором и реализован соответствующий план работ.

Результат

Основными результатами контроля защищённости ПДн будут подтверждения:

- того, что в организации построена СЗПДн, соответствующая всем требованиям (как к техническим средствам, так и к организационным процедурам), предъявляемым к ней законодательством и непосредственно самим оператором;
- того, что в течение времени, прошедшего от момента введения в эксплуатацию ИСПДн с внедрёнными в них системами и средствами защиты до момента проведения аудита, была обеспечена неизменность технологических процессов обработки защищаемой информации и других условий, способных повлиять на защищённость ПДн.

Документальными подтверждениями корректности результатов аудита служат соответствующие отчёты, заключения о результатах аудита, протоколы контроля защищённости от НСД и другие материалы инструментального контроля, а при необходимости – документированные планы совершенствования системы защиты.

Ограничения / на что стоит обратить внимание

Необходимо обратить внимание на два основных фактора, влияющих на эффективность контроля над обеспечением уровня защищённости ПДн, а именно:

- наличие полной и актуальной информации о требованиях к СЗПДн;
- обеспечение объективности результатов контроля.

Обеспечение полноты и актуальности информации

Необходимо регулярно отслеживать появление новых редакций руководящих документов, корректировок к ним, а также добиваться от представителей регулирующих органов разъяснений требований к обработке и защите ПДн.

Такая информация может быть опубликована как на официальных сайтах (Роскомнадзор – www.rsoc.ru; ФСТЭК России – www.fstec.ru; ФСБ России – www.fsb.ru), так и в других официальных источниках или выдана соответствующими ведомствами по запросу операторов или в ходе проверок.

Обеспечение объективности результатов

Необходимая объективность результатов контроля может быть обеспечена за счёт исключения из группы, проводящей аудит, специалистов, осуществлявших создание и поддержку СЗПДн.

Ссылки

- Постановление Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности ПДн при их обработке в информационных системах персональных данных»;
- BS 10012:2009 Data protection – Specification for a personal information management system;
- ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»;
- ГОСТ Р ИСО/МЭК 19011—2003 Руководящие указания по аудиту систем менеджмента качества и/или систем экологического менеджмента.

4. Заключение

Разумеется, в рамках одного подобного материала невозможно дать исчерпывающие рекомендации по реализации требований к защите ПДн в вашей организации. Кроме того, многие актуальные вопросы, связанные с данной темой, настолько сложны и узкоспециальны, что требуют сами по себе отдельного исследования.

Отметим, однако, что ряд вопросов умышленно были вынесены за рамки материала, поскольку затрагивают далеко не всех операторов ПДн. К таким вопросам можно отнести, в частности, следующие:

- особенности организации обработки ПДн при их трансграничной передаче;
- проведение аттестации сложных многопользовательских объектов информатизации, в которых ведется обработка ПДн;
- вопросы практического изменения структурной схемы хранения данных и архитектуры доступа к ним в целях снижения класса ИСПДн;
- вопросы обработки ПДн при условии их предоставления третьим лицам;
- необходимость получения лицензии ФСТЭК России на осуществление деятельности по защите конфиденциальной информации для операторов ПДн.

Кроме того, в материале не затронуты юридические аспекты защиты ПДн, которые также вызывают немало вопросов и достаточно сложны.

В целом, этот материал, как уже писалось выше, – не более чем попытка донести общую картину реализации проекта по построению СЗПДн.

Увы, всем нам постоянно приходится сталкиваться с экспертными статьями по теме защиты ПДн, в которых главное место отведено описанию противоречий норм закона действующему законодательству и трудностям реализации этих требований на практике. Действительно, можно до бесконечности обсуждать эти аспекты, откладывая при этом на будущее конкретные шаги по реализации требований законодательства о защите ПДн, которые все равно придется предпринимать, поскольку закон един для всех.

В настоящем же материале мы попытались отойти от практики фокусирования на тонких и противоречивых моментах применения законодательства о защите ПДн и дать более конструктивный взгляд, позволяющий получить достаточное количество информации о предметной области, принять решение о начале работ и перейти к конкретным действиям по реализации требований закона о защите персональных данных.

5. Список нормативно-правовых документов

1. Конвенция о защите физических лиц при автоматизированной обработке персональных данных, Страсбург, 28 января 1981 г.;
2. Федеральный закон от 02 декабря 1990 г. № 395-I «О банках и банковской деятельности»;
3. Положение по аттестации объектов информатизации по требованиям безопасности информации, утверждённое Председателем Гостехкомиссии России 25 ноября 1994 г.;
4. Гражданский кодекс Российской Федерации (ГК РФ), часть вторая, от 26 января 1996 г. № 14-ФЗ;
5. Уголовный кодекс Российской Федерации (УК РФ), от 13 июня 1996 г. № 63-ФЗ;
6. Распоряжение Президента РФ от 10 июля 2001 г. № 366-рп «О подписании Конвенции о защите физических лиц при автоматизированной обработке персональных данных»;
7. Федеральный закон от 08 августа 2001 г. № 128 «О лицензировании отдельных видов деятельности»;
8. Федеральный закон от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем»;
9. Кодекс Российской Федерации об административных правонарушениях (КоАП РФ), от 30 декабря 2001 г. № 195-ФЗ;
10. Трудовой кодекс Российской Федерации (ТК РФ), от 30 декабря 2001 г. № 197-ФЗ (гл. 14);
11. Федеральный закон от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи»;
12. Руководящий документ «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)». Утвержден приказом Гостехкомиссии России от 30 августа 2002 г. № 282 (для служебного пользования);
13. Сборник Временных методик оценки защищённости конфиденциальной информации от утечки по техническим каналам, Гостехкомиссия России, 2002 г. (для служебного пользования);
14. Федеральный закон от 07 июля 2003 г. № 126-ФЗ «О связи»;
15. Указ Президента РФ от 11 августа 2003 г. № 960 «Вопросы Федеральной службы безопасности Российской Федерации»;
16. Федеральный закон от 30 декабря 2004 г. № 218-ФЗ «О кредитных историях»;
17. Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне»;
18. Указ Президента РФ от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю»;
19. Приказ ФСБ России от 09 февраля 2005 г., Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005);
20. Указ Президента РФ от 30 мая 2005 г. № 609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела»;
21. Постановление Правительства Российской Федерации от 27 августа 2005 г. № 538 «Об утверждении Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-разыскную деятельность»;
22. Федеральный закон от 19 декабря 2005 г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»;
23. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
24. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
25. Постановление Правительства Российской Федерации от 16 августа 2006 г. № 504 «О лицензировании деятельности по технической защите конфиденциальной информации»;
26. Постановление Правительства Российской Федерации от 31 августа 2006 г. № 532 «О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации»;
27. Гражданский кодекс Российской Федерации, часть 4, от 18 декабря 2006 г. № 230-ФЗ;
28. Федеральный закон от 9 февраля 2007 г. № 16-ФЗ «О транспортной безопасности»;
29. Методический документ «Методические рекомендации по технической защите конфиденциальной информации, составляющей коммерческую тайну», ФСТЭК России, 2007 г. (для служебного пользования);

30. 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»;
31. Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России), Федеральной службы безопасности Российской Федерации (ФСБ России), Министерства информационных технологий и связи Российской Федерации (Мининформсвязи России) от 13 февраля 2008 г. № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных»;
32. Методический документ «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», ФСТЭК России, 14 февраля 2008 г. (для служебного пользования);
33. Методический документ «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», ФСТЭК России, 14 февраля 2008 г. (пометка «для служебного пользования» снята решением ФСТЭК России от 16 ноября 2009 г.);
34. Методический документ «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных», ФСТЭК России, 15 февраля 2008 г. (пометка «для служебного пользования» снята решением ФСТЭК России от 16 ноября 2009 г.);
35. Методический документ «Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», ФСТЭК России, 15 февраля 2008 г. (пометка «для служебного пользования» снята решением ФСТЭК России от 16 ноября 2009 г.);
36. 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. ФСБ России, 21 февраля 2008 г., № 149/6/6-622;
37. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации. ФСБ России, 21 февраля 2008 г, № 149/5-144;
38. Указ Президента РФ от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;
39. 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»;
40. Указ Президента РФ от 12 мая 2008 г. № 724 «Вопросы системы и структуры федеральных органов исполнительной власти»;
41. Положение о Министерстве связи и массовых коммуникаций Российской Федерации. Утверждено Постановлением Правительства РФ от 2 июня 2008 г. № 418 «О Министерстве связи и массовых коммуникаций Российской Федерации»;
42. Положение о Федеральной службе по надзору в сфере связи и массовых коммуникаций. Утверждено постановлением Правительства РФ от 2 июня 2008 г. № 419 «О Федеральной службе по надзору в сфере связи и массовых коммуникаций»;
43. Постановление Правительства Российской Федерации от 6 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;
44. Приказ Федеральной службы по надзору в сфере связи и массовых коммуникаций от 17 июля 2008 г. № 8 «Об утверждении образца формы уведомления об обработке персональных данных»;
45. Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

6. Полезные ссылки

http://leta.ru/library/search/
Правовая база, аналитика и исследования по теме защиты информации на официальном сайте LETA IT-company.

http://leta.ru/press-center/news/
Новости компании.

http://leta.ru/press-center/publications/
Статьи сотрудников LETA IT-company.

http://letablog.livejournal.com/
Блог LETA IT-company.

http://www.duma.gov.ru/csecure
Официальная страница Комитета Государственной думы по безопасности. Содержит официальные документы и информационно-аналитические материалы по вопросам информационной безопасности, в том числе по проблеме защиты персональных данных.

http://www.fsb.ru
Официальный сайт Федеральной службы безопасности Российской Федерации (ФСБ России). Содержит нормативные правовые акты, выступления руководителей службы и аналитические публикации по вопросам информационной безопасности России, в том числе по проблеме защиты персональных данных.

http://www.rsoc.ru
Официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзора), федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере информационных технологий и связи, функции по контролю и надзору за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных. Представлены нормативные правовые акты, официальные документы и аналитические публикации по вопросу защиты прав граждан при обработке персональных данных.

http://pd.rsoc.ru/press-service/subject1/news321.htm
Информационный ресурс Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзора) – «Портал персональных данных». На портале размещается информация по всему спектру деятельности Роскомнадзора в сфере защиты прав субъектов персональных данных – новости, аналитические материалы, нормативно-распорядительные документы, рекомендации для операторов персональных данных. Также через портал осуществляется доступ к реестру операторов, осуществляющих обработку персональных данных. Кроме того, «Портал персональных данных» предоставляет возможность гражданам – субъектам персональных данных получать максимум информации для отстаивания своих интересов и гражданских прав.

http://www.fstec.ru
Официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России), федерального органа исполнительной власти, осуществляющего межотраслевую координацию и функциональное регулирование деятельности по обеспечению защиты информации, содержащей сведения, составляющие государственную или служебную тайну, от её утечки по техническим каналам, от несанкционированного доступа к ней, от специальных воздействий на информацию и по

противодействию техническим средствам разведки на территории Российской Федерации. Содержит нормативные правовые акты и информационные материалы по вопросу защиты прав граждан при обработке персональных данных.

http://www.azi.ru
Сайт Межрегиональной общественной организации «Ассоциация защиты информации» (АЗИ), деятельность которой направлена на создание благоприятных условий для реализации потребностей граждан, бизнеса и органов государственной власти в продуктах и технологиях защиты информации. АЗИ активно взаимодействует с аппаратом Совета Безопасности РФ, ФСБ России, ФСТЭК России, другими министерствами и ведомствами, а также со многими финансово-экономическими структурами. Содержит нормативные правовые акты и информационные материалы по вопросу защиты персональных данных.

http://www.privacy-info.ru
Информационный проект «Персональные данные». Содержит правовые, информационно-аналитические материалы, а также новости и справочную информацию по вопросу защиты прав граждан при обработке персональных данных.

http://www.ispdn.ru
Информационный портал о защите персональных данных, представляющий «открытую площадку» для обсуждения вопросов в области защиты персональных данных, проектирования и использования информационных систем персональных данных (ИСПДн). Содержит новости по теме, аналитические публикации, правовые материалы и материалы судебной практики, форум специалистов по защите персональных данных.

http://www.infolaw.ru/position/2006-1
Электронная версия журнала «Информационное право». Представляет аналитические публикации по вопросам информационного права, в том числе создания, обработки и защиты персональных данных.

http://www.privacy-journal.ru
Сайт электронного информационно-аналитического журнала «Персональные данные», посвящённого проблематике защиты персональных данных. Предназначен для специалистов в области обработки и защиты персональных данных, а также по проблемам защиты прав граждан при обработке персональных данных.

http://www.itsec.ru/articles2/allpubliks
Электронный архив публикаций журнала «Информационная безопасность». Содержит информационно-аналитические материалы по вопросам защиты информации, в том числе защиты прав граждан при обработке персональных данных.

http://www.itsec.ru/rass.php
Архив электронной газеты «Информационная безопасность». Содержит публикации по вопросам информационной безопасности, в том числе защиты персональных данных.

http://www.secuteck.ru/articles2/allpubliks
Электронный архив публикаций журнала «Системы безопасности». Содержит информационно-аналитические материалы по вопросам защиты информации, в том числе защиты прав граждан при обработке персональных данных.

http://www.secfocus.ru
Электронный архив публикаций журнала «Security Focus», посвящённого отечественной индустрии безопасности. Содержит аналитические статьи и обзоры, нормативные правовые документы, материалы исследований, в том числе по вопросам создания, обработки и защиты персональных данных.

7. О LETA IT-company

LETA IT-company (www.leta.ru) – первый российский оператор типизированных ИТ-услуг, обеспечивающий заказчикам комплексные решения в области информационной безопасности.

Спектр услуг LETA IT-company включает все этапы жизненного цикла построения информационной безопасности на предприятии – аудит, консалтинг, внедрение, сопровождение.

В линейку услуг LETA IT-company входят как *инновационные* (**защита персональных данных**, оценка защищённости сетевых ресурсов и внедрение систем управления уязвимостями и т.д.), так и *классические* ИБ-услуги (защита информации от инсайдеров и предотвращение утечек конфиденциальных данных – DLP, построение систем ИБ по российским и международным стандартам и т.д.). Высокие компетенции LETA в различных направлениях ИБ подтверждает успешный опыт выполнения проектов. В частности, на конец 2009 года только в области защиты персональных данных портфель LETA включал более 50 проектов на разных стадиях реализации.

В рейтинге CNews Security 2009 **LETA Group**, управляющая и инвестиционная компания в сфере передовых информационных технологий, под управлением которой находится LETA IT-company, заняла **лидирующие позиции** по объёму продаж на российском рынке продуктов и услуг в сфере информационной безопасности.

Ведущие позиции LETA IT-company на рынке ИБ подтверждаются и другими достижениями:

- 1 место в рейтинге CNews «Защита информации и бизнеса от инсайдеров» (2007 год);
- 3 место в рейтинге «CNews Security 2007: крупнейшие ИТ-компании России в сфере защиты информации» (2008 год);
- победа в номинации «Системы и средства защиты информации» программы «Лучшие инновационные решения в области технологий безопасности 2007 г.» по итогам международного форума «Технологии безопасности 2007» (2007 год);
- награда «Лучшее решение в области информационной безопасности 2007» от Microsoft (2007 год).

LETA IT-company обладает лицензиями ФСТЭК России (Федеральной службы по техническому и экспортному контролю) и ФСБ России (Федеральной службы безопасности), необходимыми для деятельности в области защиты информации:

ФСТЭК России

- лицензия ФСТЭК России на деятельность по технической защите конфиденциальной информации. Регистрационный № 0943 от 30 ноября 2009 г.;
- лицензия ФСТЭК России на деятельность по разработке и (или) производству средств защиты конфиденциальной информации Регистрационный № 0571 от 30 ноября 2009 г.;

ФСБ России

- лицензия ФСБ России на осуществление разработки, производства шифровальных (криптографических) средств, защищённых с применением шифровальных (криптографических) средств информационных и телекоммуникационных систем. Рег. № 8037 П от 01 декабря 2009 г.;
- лицензия ФСБ России на осуществление технического обслуживания шифровальных (криптографических) средств. Рег. № 8038 Х от 01 декабря 2009 г.;
- лицензия ФСБ России на осуществление распространения шифровальных (криптографических) средств. Рег. № 8039 Р от 01 декабря 2009 г.;
- лицензия ФСБ России на осуществление предоставления услуг в области шифрования информации. Рег. № 8040 У от 01 декабря 2009 г.

LETA IT-company

- **входит в сообщество ABISS**, объединяющее пользователей стандартов Центрального Банка Российской Федерации по обеспечению информационной безопасности организаций банковской системы РФ
- **является сертифицированным партнером BSI** (British Standards Institution) по проведению аудита системы управления информационной безопасностью (СУИБ) первой и второй стороны, обладая статусом «BSI Certified partner».
- В рамках консорциума с компанией Digital Security, обладающей статусом QSA (Qualified Security Assessor), LETA IT-company оказывает заказчикам полный комплекс услуг по выполнению требований стандарта PCI DSS.

В рамках многолетнего сотрудничества LETA IT-company обладает высокими партнерскими статусами у ведущих мировых и российских разработчиков, в частности:

- *Platinum Partner* от **Symantec**,
- *Gold ChannelConnect Partner* от **Websense**,
- *Security Alliance Elite Partner* от **McAfee**,
- *AffinityPlus Partner* от **Trend Micro**,
- *Bronze Partner* от **Check Point**,
- *Gold Certified Partner от* **Microsoft** (с компетенцией *«Security Solutions»* в числе других)

и т.д.

LETA IT-company входит в состав LETA Group – управляющую компанию в сфере передовых информационных технологий, наряду с LETA IT-company объединяющую компании ESET, ACK, «Дамаск», MrSoft, Veyer.

LETA IT-company

109129, Москва, ул. 8-я Текстильщиков, д. 11, стр. 2

Тел./факс: +7 (495) 921 1410

e-mail: info@leta.ru, http://www.leta.ru